Рег. № ПО-16-1033
Дата: 20.08.2020

ДОГОВОР

Днес,.....2020 г., в гр. София, между:

„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ" АД, ЕИК: 831641791, със седалище и адрес на управление: гр. София 1504, район „Оборище", ул. „Панайот Волов"№ 2, представлявано от Ивайло Филипов – изпълнителен директор на дружеството, в качеството му на системен интегратор по чл. 7с от Закона за електронното управление и публичен възложител на обществени поръчки по смисъла на § 45, ал. 1 от Преходните и заключителни разпоредби към Закона за изменение и допълнение на Закона за електронното управление, наричано по-долу за краткост **ВЪЗЛОЖИТЕЛ**, от една страна,

И

„КОНТРАКС" АД, със седалище и адрес на управление: гр. София, п.к. 1113 „Изгрев", ул. „Тинтява" № 13, ЕИК/БУЛСТАТ: 175415627, представлявано от Николай Йорданов – изпълнителен директор, наричан по-нататък за краткост **„ИЗПЪЛНИТЕЛ"**

(**ВЪЗЛОЖИТЕЛЯТ** и **ИЗПЪЛНИТЕЛЯТ** наричани заедно „Страните", а всеки от тях поотделно „Страна")

на основание чл. 112 от Закона за обществените поръчки (ЗОП), във връзка с чл. 69 от Правилника за прилагане на Закона за обществените поръчки (ППЗОП), след проведена „открита" процедура за възлагане на обществена поръчка с предмет **„Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите"**
и въз основа на Решение № 51-00-30-19/31.07.2020 г. на изпълнителния директор на „Информационно обслужване" АД за определяне на изпълнител на обществена поръчка по обособена позиция № 7 с предмет: „Доставка на система за защита от изтичане/загуба на данни от крайните точки и от мрежата" (*попълва се за съответната позиция, за която участникът е избран за изпълнител)*, се сключи този договор (**„Договора/Договорът"**) за възлагане на обществена поръчка.

Страните се споразумяха за следното:

Заличаванията на информация в документа са на основание чл. 4 от Общ регламент за защита на данните

I. ПРЕДМЕТ НА ДОГОВОРА

Чл. 1. (1) **ВЪЗЛОЖИТЕЛЯТ** възлага, а **ИЗПЪЛНИТЕЛЯТ** приема срещу възнаграждение да осъществи следните дейности:

1. доставка на софтуер, необходим за обновяване на информационни и комуникационни системи на Национална агенция по приходите (наричано по-нататък за краткост „софтуер" или „доставките"), подробно описан по вид, количество и технически характеристики в Техническата спецификация на **ВЪЗЛОЖИТЕЛЯ** с предмет: „Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите" – Приложение № 1 (наричана по-нататък „Техническа спецификация"), Приложение към нея, относимо към обособена позиция № 7 с предмет „Доставка на система за защита от изтичане/загуба на данни от крайните точки и от мрежата" - Приложение № 1.7 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)* и Техническото предложение на **ИЗПЪЛНИТЕЛЯ** по обособена позиция № 7 – Приложение № 2.7 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)*, представляващи неразделна част от настоящия договор.

2. гаранционно обслужване на доставения софтуер по т. 1 (наричано алтернативно „гаранция и поддръжка"), осигурено в рамките на срока по чл. 4, ал. 3 в съответствие с предписанията на производителя, изискванията на настоящия договор и приложенията към него.

(2) Доставката на софтуера по ал. 1, т. 1 се извършва от **ИЗПЪЛНИТЕЛЯ** въз основа на писмена заявка до **ИЗПЪЛНИТЕЛЯ**, отправена чрез адреса за кореспонденция на хартиен носител, или по електронна поща, подписана с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис на **ВЪЗЛОЖИТЕЛЯ** или упълномощен негов представител, съгласно клаузите на този договор. В писмената заявка се посочват:

1. Вид и обем на софтуера, който следва да бъде доставен;

2. Място на доставка;

3. Срок на доставка, съобразен със сроковете и условията на доставка по настоящия договор.

4. Друга информация по преценка на **ВЪЗЛОЖИТЕЛЯ**, относима към изпълнението на договора.

II. ЦЕНИ И НАЧИН НА ПЛАЩАНЕ

Чл. 2. (1) Общата цена по договора е в размер на 1 684 045.00 лева (един милион шестстотин осемдесет и четири хиляди четиридесет и пет лева и нула стотинки) без ДДС, съгласно Ценовото предложение на **ИЗПЪЛНИТЕЛЯ** – Приложение № 3.7 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)*, неразделна част от настоящия договор.

(2) **ВЪЗЛОЖИТЕЛЯТ** заплаща на **ИЗПЪЛНИТЕЛЯ** цената за изпълнената доставка съобразно цените на доставения и приет софтуер, посочени в Ценовото предложение на **ИЗПЪЛНИТЕЛЯ** – Приложение № 3.7 към настоящия договор (*попълва се за съответната позиция, за която участникът е избран за изпълнител).*

(3) В цените по ал. 2, съответно в общата цена по ал. 1, са включени всички разходи на **ИЗПЪЛНИТЕЛЯ** по изпълнението на договора, като **ВЪЗЛОЖИТЕЛЯТ** не дължи заплащането на каквито и да е други разноски по договора.

(4) Цените по ал. 2, съответно общата цена по ал. 1, посочени в Ценовото предложение на **ИЗПЪЛНИТЕЛЯ** – Приложение № 3.7 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)* са крайни и не могат да бъдат променяни за срока на договора, освен в случаите, когато промяната е в полза на **ВЪЗЛОЖИТЕЛЯ,** както и при спазване на реда и условията на ЗОП.

Чл. 3. (1) Плащането се извършва в срок до 30 (тридесет) дни след представяне на следните документи:

1. Двустранно подписан приемо-предавателен протокол за извършена доставка по чл. 6, ал. 1; съответно чл. 6, ал. 2, когато е приложимо.

2. Оригинална фактура, предоставена от **ИЗПЪЛНИТЕЛЯ**, която съдържа подробна разбивка по единични цени, по услуги и видове за всеки един компонент, съдържащ се в доставения софтуер.

(2) Плащането се спира, когато **ИЗПЪЛНИТЕЛЯТ** бъде уведомен, че фактурата му не може да бъде платена, тъй като сумата не е дължима поради липсващи и/или некоректни придружителни документи или наличие на доказателства, че разходът е неправомерен. В този случай, **ИЗПЪЛНИТЕЛЯТ** трябва да даде разяснения, да направи изменения или представи допълнителна информация в срок до 3 (три) работни дни, след като бъде уведомен за това. В този случай срокът за извършване на плащане към **ИЗПЪЛНИТЕЛЯ** започва да тече от датата на която **ВЪЗЛОЖИТЕЛЯТ** получи правилно оформена фактура и/или поисканите разяснения, корекции и/или допълнителна информация.

(3) Плащанията се извършват от **ВЪЗЛОЖИТЕЛЯ** в български левове, с платежно нареждане по банкова сметка, посочена от **ИЗПЪЛНИТЕЛЯ**, както следва:

Банка: „УниКредит Булбанк" АД

IBAN: BG45UNCR96601034361601

BIC: UNCRBGSF

(4) **ИЗПЪЛНИТЕЛЯТ** е длъжен да уведомява писмено **ВЪЗЛОЖИТЕЛЯ** за всички последващи промени по ал. 3 в срок до 3 (три) дни, считано от момента на промяната. В случай че

ИЗПЪЛНИТЕЛЯТ не уведоми **ВЪЗЛОЖИТЕЛЯ** в този срок, счита се, че плащанията са надлежно извършени.

(5) Когато **ИЗПЪЛНИТЕЛЯТ** е сключил договор/договори за подизпълнение, **ВЪЗЛОЖИТЕЛЯТ** извършва окончателно плащане към него, след като бъдат представени доказателства, че **ИЗПЪЛНИТЕЛЯТ** е заплатил на подизпълнителя/подизпълнителите за изпълнените от тях работи, които са приети по реда на раздел IV и са спазени условията на раздел IXа от настоящия договор.

III. СРОК И МЯСТО ЗА ИЗПЪЛНЕНИЕ

Чл. 4. (1) Договорът влиза в сила от датата на подписването му от двете страни и действието му се прекратява с изтичането на срока на гаранционното обслужване, посочен в ал. 3. Датата на подписване е датата, посочена в деловодния номер на **ВЪЗЛОЖИТЕЛЯ**, поставен на стр. 1 от настоящия договор.

(2) Срокът на извършване на доставката на софтуера е 10 (десет) календарни дни *(до 80 календарни дни съгласно изискванията на документацията за обществената поръчка по съответната обособена позиция)* от получаване на писмената заявка по чл. 1, ал. 2 от **ВЪЗЛОЖИТЕЛЯ**.

(3) Срокът на гаранционно обслужване на доставения софтуер е 5 години *(минимум 5 (пет) години съгласно изискванията на документацията за обществената поръчка по съответната обособена позиция)* и започва да тече от датата на подписване на двустранен приемо-предавателен протокол за приемане на доставката.

Чл. 5. (1) Мястото на извършване на доставката е на територията на гр. София, като **ВЪЗЛОЖИТЕЛЯТ** ще посочи в писмената заявка по чл. 1, ал. 2 конкретния адрес на извършване на доставката.

(2) Гаранционното обслужване ще се извършва по местонахождението на доставения и инсталиран софтуер.

IV. УСЛОВИЯ НА ДОСТАВКА. ПРЕДАВАНЕ И ПРИЕМАНЕ НА ИЗПЪЛНЕНИЕТО

Чл. 6. (1) Приемането на всяка конкретна доставка на софтуера се удостоверява с двустранен приемо-предавателен протокол, който се подписва от упълномощените представители на страните по договора. При извършване на доставката на софтуер, **ИЗПЪЛНИТЕЛЯТ** представя на **ВЪЗЛОЖИТЕЛЯ** необходимите сертификати или други документи, удостоверяващи предоставеното право на ползване на софтуера. („**Приемо-предавателен протокол за доставка на софтуер**").

(2) При констатиране на явни недостатъци, повреди, дефекти, липси, и/или несъответствия на доставения софтуер с Техническата спецификация – Приложение № 1, Приложение № 1.7 към нея

(попълва се за съответната позиция, за която участникът е избран за изпълнител) или Техническото предложение – Приложение № 2.7 *(попълва се за съответната позиция, за която участникът е избран за изпълнител)* при извършване на прегледа по ал. 2, **ВЪЗЛОЖИТЕЛЯТ** има право да откаже да подпише съответния приемо-предавателен протокол. В тези случаи страните подписват двустранен констативен протокол, в който се описват констатираните недостатъци, повреди, дефекти, липси и/или несъответствия и се посочва срокът, в който същите да бъдат отстранени (**„Констативен протокол за липса на съответствие“**). След отстраняването им страните подписват двустранен приемо-предавателен протокол по реда и условията на ал. 1 за приемане на доставката.

(3) Когато **ИЗПЪЛНИТЕЛЯТ** е сключил договор/договори за подизпълнение, работата на подизпълнителя/подизпълнителите се приема от **ВЪЗЛОЖИТЕЛЯ** в присъствието на **ИЗПЪЛНИТЕЛЯ** и подизпълнителя/подизпълнителите.

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА СТРАНИТЕ ПО ДОГОВОРА

Чл. 7. Изброяването на конкретни права и задължения на страните в този раздел от договора е неизчерпателно и не засяга действието на други клаузи от договора или от приложимото право, предвиждащи права и/или задължения на която и да е от страните.

Чл. 8. ВЪЗЛОЖИТЕЛЯТ има право да:

1. изисква от **ИЗПЪЛНИТЕЛЯ** да получи изпълнение съгласно условията на настоящия договор и приложенията към него;

2. извършва проверка във всеки момент от изпълнението на договора относно качество, обем, стадий на изпълнение, технически параметри без с това да пречи на оперативната дейност на **ИЗПЪЛНИТЕЛЯ**;

3. изисква от **ИЗПЪЛНИТЕЛЯ** да сключи и да му представи договори за подизпълнение с посочените в офертата му подизпълнители.

Чл. 9. ВЪЗЛОЖИТЕЛЯТ е длъжен да:

1. оказва необходимото съдействие на **ИЗПЪЛНИТЕЛЯ** за изпълнение на задълженията, произтичащи от договора;

2. приеме доставения софтуер при качествено и точно изпълнение на задълженията от страна на **ИЗПЪЛНИТЕЛЯ**;

3. да използва доставения софтуер съобразно предназначението му и предписанията на производителя;

4. да заплати цената при извършване на доставката при качествено и точно изпълнение на задълженията, съгласно клаузите на настоящия договор.

Чл. 10. ИЗПЪЛНИТЕЛЯТ има право:

1. при пълно, точно и навременно изпълнение на задълженията си да получи уговореното възнаграждение при условията и в сроковете, посочени в настоящия договор;

2. да иска от **ВЪЗЛОЖИТЕЛЯ** необходимото съдействие за осъществяване на задълженията си по договора;

3. да иска от **ВЪЗЛОЖИТЕЛЯ** приемане на доставката, когато тя отговаря на изискванията, посочени в настоящия договор и приложенията към него.

Чл. 11. ИЗПЪЛНИТЕЛЯТ е длъжен да:

1. изпълни поръчката, предмет на настоящия договор, в срок и качествено, в съответствие с изискванията на Техническата спецификация и Техническото предложение, които представляват неразделна част от настоящия договор;

2. информира текущо **ВЪЗЛОЖИТЕЛЯ** за хода на изпълнението на настоящия договор и да го уведомява за всяко възникнало събитие, което би довело до забава и/или неизпълнение на задължение по договора и да предложи мерки за неговото преодоляване;

3. да извършва гаранционно обслужване на доставения софтуер съгласно предписанията на производителя, изискванията на настоящия договор и приложенията към него,

4. да предоставя всички нови версии на софтуерните продукти, с оказване на необходимото съдействие на **ВЪЗЛОЖИТЕЛЯ** за изтеглянето им и за работата с тях;

5. да предоставя информация по запитвания и заявки от страна на **ВЪЗЛОЖИТЕЛЯ** във връзка с ползването на продуктите;

5.1. да оказва висококвалифицирана специализирана помощ и съдействие за отстраняването на възникнали инциденти и проблеми;

5.2. да отстранява възникнали грешки в софтуера и своевременното да го обновява;

5.3. да осигури свободно и безпрепятствено ползване на продуктите за срока на действие на доставените за тях лицензи *(когато е приложимо)*.

6. да уведоми незабавно **ВЪЗЛОЖИТЕЛЯ** при възникване на пречки от стопански, административен или друг характер, които могат да забавят или да направят невъзможно изпълнението на този договор, като може да поиска от **ВЪЗЛОЖИТЕЛЯ** указания и/или съдействие за отстраняването им.

VI. ГАРАНЦИЯ ЗА ИЗПЪЛНЕНИЕ

Чл. 12. (1) При подписването на този договор, **ИЗПЪЛНИТЕЛЯТ** предоставя на **ВЪЗЛОЖИТЕЛЯ** гаранция за изпълнение в размер на 1% (едно на сто) от стойността по чл. 2, ал. 1.

(**„Гаранцията за изпълнение“**) или **16 840,45 лв.** (шестнадесет хиляди осемстотин и четиридесет лева четиридесет и пет стотинки).

(2) Гаранцията за изпълнение е предназначена за обезпечаване на задълженията на **ИЗПЪЛНИТЕЛЯ** по договора, както следва:

1. 50% от сумата по ал. 1 – за изпълнение на дейностите по доставка на софтуер;

2. 50 % от сумата по ал. 1 – за изпълнение на дейностите по гаранционно обслужване.

(3) **ИЗПЪЛНИТЕЛЯТ** избира формата на гаранцията в една от следните форми:

1. парична сума внесена по банковата сметка на Възложителя;

2. банкова гаранция; или

3. застраховка, която обезпечава изпълнението чрез покритие на отговорността на **ИЗПЪЛНИТЕЛЯ.**

Чл. 13. (1) В случай на изменение на договора, извършено в съответствие с този договор и приложимото право, **ИЗПЪЛНИТЕЛЯТ** се задължава да предприеме необходимите действия за привеждане на Гаранцията за изпълнение в съответствие с изменените условия на договора, в срок до 3 (три) работни дни от подписването на допълнително споразумение за изменението.

(2) Действията за привеждане на Гаранцията за изпълнение в съответствие с изменените условия на договора могат да включват, по избор на **ИЗПЪЛНИТЕЛЯ**:

1. внасяне на допълнителна парична сума по банковата сметка на **ВЪЗЛОЖИТЕЛЯ**, при спазване на чл. 14 от договора; и/или;

2. предоставяне на документ за изменение на първоначалната банкова гаранция или нова банкова гаранция, при спазване на изискванията на чл. 15 от договора; и/или

3. предоставяне на документ за изменение на първоначалната застраховка или нова застраховка, при спазване на изискванията на чл. 16 от договора.

Чл. 14. (1) Когато гаранцията се предоставя във вид на парична сума, тя се внася по следната банкова сметка на **ВЪЗЛОЖИТЕЛЯ:**

IBAN: BG43CECB979010C7866100;

BIC: CECBBGSF

Банка: „Централна кооперативна банка“ АД

(2) Всички банкови разходи, свързани с преводите на сумата са за сметка на **ИЗПЪЛНИТЕЛЯ**.

Чл. 15. (1) Когато като гаранция за изпълнение се представя банкова гаранция, **ИЗПЪЛНИТЕЛЯТ** предава на **ВЪЗЛОЖИТЕЛЯ** оригинален екземпляр на банкова гаранция, издадена в полза на **ВЪЗЛОЖИТЕЛЯ**, която трябва да отговаря на следните изисквания:

1. да бъде безусловна и неотменяема банкова гаранция във форма, предварително съгласувана с **ВЪЗЛОЖИТЕЛЯ**, и да съдържа задължение на банката-гарант да извърши плащане

при първо писмено искане от **ВЪЗЛОЖИТЕЛЯ**, деклариращ, че е налице неизпълнение на задължение на **ИЗПЪЛНИТЕЛЯ** или друго основание за задържане на Гаранцията за изпълнение по този договор;

2. да бъде със срок на валидност за целия срок на действие на договора, плюс 30 (тридесет) дни, като при необходимост срокът на валидност на банковата гаранция се удължава или се издава нова.

(2) Всички банкови разходи свързани с откриването и обслужването на банковата гаранция, по усвояването на средства от страна на **ВЪЗЛОЖИТЕЛЯ**, при наличието на основание за това, както и при нейното връщане са за сметка на **ИЗПЪЛНИТЕЛЯ**.

Чл. 16. (1) Когато като Гаранция за изпълнение се представя застраховка, **ИЗПЪЛНИТЕЛЯТ** предава на **ВЪЗЛОЖИТЕЛЯ** оригинален екземпляр на застрахователна полица, предварително съгласувана с **ВЪЗЛОЖИТЕЛЯ**, издадена в полза на **ВЪЗЛОЖИТЕЛЯ**, в която **ВЪЗЛОЖИТЕЛЯТ** е посочен като трето ползващо се лице (бенефициер), която трябва да отговаря на следните изисквания:

1. да обезпечава изпълнението на този договор чрез покритие на отговорността на **ИЗПЪЛНИТЕЛЯ** в определения в чл. 12, ал. 1 размер;

2. да бъде със срок на валидност за целия срок на действие на договора, плюс 30 (тридесет) дни, като при необходимост срокът на валидност на гаранцията се удължава или се издава нова.

3. Застрахователната премията по застраховката следва да е платена на сто процента (не се допуска разсрочено заплащане на застрахователната премия) и не може да бъде използвана за обезпечение на отговорността на изпълнителя по друг договор.

(2) Разходите по сключването на застрахователния договор и поддържането на валидността на застраховката за изисквания срок, както и по всяко изплащане на застрахователно обезщетение в полза на **ВЪЗЛОЖИТЕЛЯ**, при наличието на основание за това, са за сметка на **ИЗПЪЛНИТЕЛЯ**

Чл. 17. **(1) ВЪЗЛОЖИТЕЛЯТ** освобождава гаранцията за изпълнение, както следва:

1. Сумата по чл. 12, ал. 2, т. 1 се освобождава в срок до 30 (тридесет) дни след окончателното приемане на доставката, ако липсват основания за задържането от страна на **ВЪЗЛОЖИТЕЛЯ**, на каквато и да е сума по нея.

2. Сумата по чл. 12, ал. 2, т. 2 се освобождава в срок до 30 (тридесет) дни след изтичане на срока на гаранционното обслужване, в случай, че липсват основания за задържането от страна на **ВЪЗЛОЖИТЕЛЯ**, на каквато и да е сума по нея.

(2) Освобождаването на Гаранцията за изпълнение се извършва, както следва:

1. когато е във формата на парична сума – чрез превеждане на сумата по банковата сметка на **ИЗПЪЛНИТЕЛЯ**, посочена в чл. 12, ал. 1 от договора;

2. когато е във формата на банкова гаранция – чрез връщане на нейния оригинал на представител на **ИЗПЪЛНИТЕЛЯ** или упълномощено от него лице;

3. когато е във формата на застраховка – чрез връщане на оригинала на застрахователната полица/застрахователния сертификат на представител на **ИЗПЪЛНИТЕЛЯ** или упълномощено от него лице.

(3) Гаранцията или съответната част от нея не се освобождава от **ВЪЗЛОЖИТЕЛЯ**, ако в процеса на изпълнение на договора е възникнал спор между Страните относно неизпълнение на задълженията на **ИЗПЪЛНИТЕЛЯ** и въпросът е отнесен за решаване пред съд. При решаване на спора в полза на **ВЪЗЛОЖИТЕЛЯ** той може да пристъпи към усвояване на гаранциите.

Чл. 18. **ВЪЗЛОЖИТЕЛЯТ** има право да задържи съответна част и да се удовлетвори от Гаранцията за изпълнение, когато **ИЗПЪЛНИТЕЛЯТ** не изпълни някое от неговите задължения по договора, както и в случаите на лошо, частично и забавено изпълнение на което и да е задължение на **ИЗПЪЛНИТЕЛЯ**, като усвои такава част от Гаранцията за изпълнение, която съответства на уговорената в договора неустойка за съответния случай на неизпълнение.

Чл. 19. **ВЪЗЛОЖИТЕЛЯТ** има право да задържи Гаранцията за изпълнение в пълен размер, в следните случаи:

1. при пълно неизпълнение и разваляне на договора от страна на **ВЪЗЛОЖИТЕЛЯ** на това основание;

2. при прекратяване на дейността на **ИЗПЪЛНИТЕЛЯ** или при обявяването му в несъстоятелност.

Чл. 20. Във всеки случай на задържане на Гаранцията за изпълнение, **ВЪЗЛОЖИТЕЛЯТ** уведомява **ИЗПЪЛНИТЕЛЯ** за задържането и неговото основание. Задържането на Гаранцията за изпълнение изцяло или частично не изчерпва правата на **ВЪЗЛОЖИТЕЛЯ** да търси обезщетение в по-голям размер.

Чл. 21. Когато **ВЪЗЛОЖИТЕЛЯТ** се е удовлетворил от Гаранцията за изпълнение и договорът продължава да е в сила, **ИЗПЪЛНИТЕЛЯТ** се задължава в срок до 5 (пет) дни да допълни Гаранцията за изпълнение, като внесе усвоената от **ВЪЗЛОЖИТЕЛЯ** сума по сметката на **ВЪЗЛОЖИТЕЛЯ** или предостави документ за изменение на първоначалната банкова гаранция или нова банкова гаранция, съответно застраховка, така че във всеки момент от действието на договора размерът на Гаранцията за изпълнение да бъде в съответствие с чл. 12, ал. 1 от договора.

Чл. 22. **ВЪЗЛОЖИТЕЛЯТ** не дължи лихва за времето, през което средствата по Гаранцията за изпълнение са престояли при него законосъобразно.

VII. ГАРАНЦИОННО ОБСЛУЖВАНЕ

Чл. 23. (1) **ИЗПЪЛНИТЕЛЯТ** гарантира за срока, посочен в чл. 4, ал. 3, пълната функционална годност на доставения софтуер съгласно предписанията на производителя, изискванията на настоящия договор и приложенията към него.

(2) В рамките на срока по ал. 1 **ИЗПЪЛНИТЕЛЯТ** отстранява за своя сметка всички повреди и/или несъответствия на софтуера.

Чл. 24. (1) **ИЗПЪЛНИТЕЛЯТ** се задължава да предоставя обобщен отчет за извършените дейности по гаранционно обслужване на всяко тримесечие, които се приемат от **ВЪЗЛОЖИТЕЛЯ**. В обобщените отчети се посочва най-малко следната информация: период на покритие на отчета и списък с възникналите проблеми и параметрите, при които **ИЗПЪЛНИТЕЛЯТ** е отстранил проблемите.

(2) В случай, че **ВЪЗЛОЖИТЕЛЯТ** има забележки по представения отчет по ал. 1, **ВЪЗЛОЖИТЕЛЯТ** може да откаже да го подпише. В този случай **ВЪЗЛОЖИТЕЛЯТ** уведомява писмено **ИЗПЪЛНИТЕЛЯ** и в срок до 10 (десет) работни дни от получаване на уведомлението, страните подписват констативен протокол, в който се отразяват направените забележки и се определя срок за тяхното отстраняване. В случай че **ИЗПЪЛНИТЕЛЯТ** откаже да подпише констативния протокол **ВЪЗЛОЖИТЕЛЯТ** има право сам да състави такъв протокол като съдържанието му е задължително за **ИЗПЪЛНИТЕЛЯ**. Приемането се извършва след отстраняване на забележките в установения срок с подписването на коригиран отчет.

(3) Ако забележките не бъдат отстранени в установения срок, **ВЪЗЛОЖИТЕЛЯТ** може да развали договора с едностранно уведомление, отправено до другата страна, без да дава допълнителен срок за изпълнение.

VIII. НЕУСТОЙКИ

Чл. 25. (1) При забавено изпълнение на задължения по договора от страна на **ИЗПЪЛНИТЕЛЯ** в нарушение на уговорените в този договор срокове, същият заплаща на **ВЪЗЛОЖИТЕЛЯ** неустойка в размер на 0,1 % (нула цяло и една десета на сто) от сумата по чл. 2, ал. 1, за всеки просрочен ден, но не повече от 3 % (три на сто) от тази сума.

(2) При забава на **ВЪЗЛОЖИТЕЛЯ** за изпълнение на задълженията му за плащане по договора, същият заплаща на **ИЗПЪЛНИТЕЛЯ** неустойка в размер на 0,1 % (нула цяло и една десета на сто) от сумата по чл. 2, ал. 1, за всеки просрочен ден, но не повече от 3 % (три на сто) от тази сума.

IX. НЕУСТОЙКИ

Чл. 26. (1) При пълно неизпълнение на договора от страна на **ИЗПЪЛНИТЕЛЯ, ВЪЗЛОЖИТЕЛЯТ** усвоява предоставената гаранция за изпълнение.

(2) При забавено изпълнение на задължения по договора от страна на **ИЗПЪЛНИТЕЛЯ** в нарушение на уговорените в този договор срокове, същият заплаща на **ВЪЗЛОЖИТЕЛЯ** неустойка в размер на 0,1 % (нула цяло и една десета на сто) от сумата по чл. 2, ал. 1, за всеки просрочен ден.

(3) При забава на **ВЪЗЛОЖИТЕЛЯ** за изпълнение на задълженията му за плащане по договора, същият заплаща на **ИЗПЪЛНИТЕЛЯ** неустойка в размер на 0,1 % (нула цяло и една десета на сто) от сумата по чл. 2, ал. 1, за всеки просрочен ден, но не повече от 3 на сто (три на сто) от тази сума.

(4) При системно (три и повече пъти) неизпълнение на задълженията за сервизно обслужване в гаранционния срок, **ИЗПЪЛНИТЕЛЯТ** дължи на **ВЪЗЛОЖИТЕЛЯ**, неустойка в размер на 0.5 (нула цяло и пет десети на сто) на сто от сумата по чл. 2, ал. 1.

Чл. 27. **ВЪЗЛОЖИТЕЛЯТ** може да претендира обезщетение за нанесени вреди и пропуснати ползи по общия ред, независимо от начислените неустойки и независимо от усвояването на гаранцията за изпълнение.

IXa. ПОДИЗПЪЛНИТЕЛИ (когато е приложимо)[1]

Чл. 27а. (1) **ИЗПЪЛНИТЕЛЯТ** е длъжен в срок от три дни от сключването на договор за подизпълнение, както и на допълнително споразумение за замяна на посочен в офертата подизпълнител, да изпрати на **ВЪЗЛОЖИТЕЛЯ** копие на договора/допълнителното споразумение, заедно с доказателства, че са изпълнени условията на чл. 66, ал. 2 или ал. 14 от ЗОП.

(2) **ИЗПЪЛНИТЕЛЯТ** носи пълна отговорност за действията и/или бездействията на подизпълнителите си, като участието им при изпълнението на поръчката, не изменя или намалява задълженията на **ИЗПЪЛНИТЕЛЯ**, съгласно настоящия договор. Видът и делът на участието на подизпълнителя/те следва да бъдат същите, като посочените в офертата на **ИЗПЪЛНИТЕЛЯ.**

(3) При сключването на договор/и с подизпълнител/и, оферирани в офертата на **ИЗПЪЛНИТЕЛЯ,** последният е длъжен да създаде условия, че:

1. приложимите клаузи на договора са задължителни за изпълнение от подизпълнителя/ите;

2. действията на подизпълнителя/ите няма да доведат пряко или косвено до неизпълнение на договора, за което **ИЗПЪЛНИТЕЛЯТ** да иска освобождаването си от отговорност;

[1] Изискванията и условията, предвидени в този раздел се прилагат в случаите, когато Изпълнителят е предвидил използването на подизпълнители

3. при осъществяване на правата си по настоящия договор, **ВЪЗЛОЖИТЕЛЯТ** ще може без ограничения да извършва проверка на дейността и документацията на подизпълнителя/ите;

4. подизпълнителят няма право да превъзлага една или повече от дейностите, които са включени в предмета на договора за подизпълнение.

(4) **ИЗПЪЛНИТЕЛЯТ** може да извършва замяна на посочените подизпълнители за изпълнение на договора, както и да включва нови подизпълнители в предвидените в ЗОП случаи и при предвидените в ЗОП условия.

(5) Сключването на договор с подизпълнител, който не е обявен в офертата на **ИЗПЪЛНИТЕЛЯ** и не е включен по време на изпълнение на договора по предвидения в ЗОП ред или изпълнението на дейностите по договора от лице, което не е подизпълнител, обявено в офертата на **ИЗПЪЛНИТЕЛЯ**, се счита за неизпълнение на договора и е основание за едностранно прекратяване на договора от страна на Възложителя и за усвояване на пълния размер на гаранцията за изпълнение.

(6) Независимо от използването на подизпълнители, отговорността за изпълнение на настоящия договор е на **ИЗПЪЛНИТЕЛЯ.**

Чл. 27б. (1) Когато частта от поръчката, която се изпълнява от подизпълнител, може да бъде предадена като отделен обект на **ИЗПЪЛНИТЕЛЯ** или на **ВЪЗЛОЖИТЕЛЯ**, **ВЪЗЛОЖИТЕЛЯТ** заплаща възнаграждение за тази част директно на подизпълнителя.

(2) Разплащанията по ал. 1 се осъществяват въз основа на искане, отправено от подизпълнителя до **ВЪЗЛОЖИТЕЛЯ** чрез **ИЗПЪЛНИТЕЛЯ**, който е длъжен да го предостави на **ВЪЗЛОЖИТЕЛЯ** в 15-дневен срок от получаването му.

(3) Към искането по ал. 2 **ИЗПЪЛНИТЕЛЯТ** предоставя становище, от което да е видно дали оспорва плащанията или част от тях като недължими.

(4) **ВЪЗЛОЖИТЕЛЯТ** има право да откаже плащане по ал. 2, когато искането за плащане е оспорено, до момента на отстраняване на причината за отказа.

X. ПРЕКРАТЯВАНЕ И РАЗВАЛЯНЕ НА ДОГОВОРА

Чл. 28. (1) Настоящият договор се прекратява:

1. с изпълнение на всички задължения на страните по договора;

2. при настъпване на обективна невъзможност за изпълнение на договора, включително отмяна на изключителните права на системния интегратор за изпълнение на съответните дейности, посредством промяна в нормативната уредба.

3. при настъпване на друга невиновна невъзможност за изпълнение, непредвидено или непредотвратимо събитие от извънреден характер, възникнало след сключването на договора („непреодолима сила"), продължила повече от 45 дни;

4. при прекратяване на юридическо лице – Страна по договора без правоприемство, по смисъла на законодателството на държавата, в която съответното лице е установено;

5. при условията по чл. 5, ал. 1, т. 3 от Закона за икономическите и финансовите отношения с дружествата, регистрирани в юрисдикции с преференциален данъчен режим, контролираните от тях лица и техните действителни собственици.

(2) Настоящият договор може да бъде прекратен:

1. по взаимно съгласие на Страните, изразено в писмена форма;

2. когато за **ИЗПЪЛНИТЕЛЯ** бъде открито производство по несъстоятелност или ликвидация – по искане на **ВЪЗЛОЖИТЕЛЯ;**

Чл. 29. ВЪЗЛОЖИТЕЛЯТ прекратява договора в случаите по чл. 118, ал. 1 от ЗОП, без да дължи обезщетение на **ИЗПЪЛНИТЕЛЯ** за претърпени от прекратяването на Договора вреди, освен ако прекратяването е на основание чл. 118, ал. 1, т. 1 от ЗОП. (В последния случай размерът на обезщетението се определя в протокол или споразумение, подписано от Страните, а при непостигане на съгласие – по реда на клаузата за разрешаване на спорове по този договор.)

Чл. 30. (1) Всяка от страните може да развали договора при виновно неизпълнение на съществено задължение на другата страна по договора, при условията и с последиците съгласно чл. 87 и сл. от Закона за задълженията и договорите, чрез отправяне на писмено предупреждение от изправната страна до неизправната и определяне на подходящ срок за изпълнение. Разваляне на договора не се допуска, когато неизпълнената част от задължението е незначителна с оглед на интереса на изправната страна.

(2) По смисъла на този договор „виновно неизпълнение на съществено задължение на **ИЗПЪЛНИТЕЛЯ**" е:

1. когато **ИЗПЪЛНИТЕЛЯТ** забави изпълнението на задължение по настоящия договор с повече от 30 (тридесет) календарни дни;

2. при системно (три или повече пъти) неизпълнение на задълженията на **ИЗПЪЛНИТЕЛЯ** за гаранционно обслужване и при пълно неизпълнение на задълженията на **ИЗПЪЛНИТЕЛЯ** за гаранционно обслужване;

3. когато **ИЗПЪЛНИТЕЛЯТ** използва подизпълнител, без да е декларирал това в офертата си.

Чл. 31. При предсрочно прекратяване на договора, **ВЪЗЛОЖИТЕЛЯТ** е длъжен да заплати на **ИЗПЪЛНИТЕЛЯ** реално изпълнените и приети по установения ред доставки/услуги.

XI. НЕПРЕОДОЛИМА СИЛА

Чл. 32. (1) Страните се освобождават от отговорност за неизпълнение на задълженията си, когато невъзможността за изпълнение се дължи на непреодолима сила. Никоя от страните не може

да се позовава на непреодолима сила, ако е била в забава и не е информирала другата страна за възникването на непреодолима сила.

(2) Страната, засегната от непреодолима сила, е длъжна да предприеме всички разумни усилия и мерки, за да намали до минимум понесените вреди и загуби, както и да уведоми писмено другата страна незабавно при настъпване на непреодолимата сила.

(3) Докато трае непреодолимата сила, изпълнението на задължението се спира.

(4) Не може да се позовава на непреодолима сила онази страна, чиято небрежност или умишлени действия или бездействия са довели до невъзможност за изпълнение на договора.

XII. КОНФИДЕНЦИАЛНОСТ

Чл. 33. (1) Всяка от страните по този договор се задължава да пази в поверителност и да не разкрива или разпространява информация за другата страна, станала ▯ известна при или по повод изпълнението на договора („**Конфиденциална информация**“) включително и след прекратяването на същия, неограничено във времето. Конфиденциална информация включва, без да се ограничава до: всякаква финансова, търговска, техническа или друга информация, анализи, съставени материали, изследвания, документи или други материали, свързани с бизнеса, управлението или дейността на другата Страна, от каквото и да е естество, или в каквато и да е форма, включително финансови и оперативни резултати, пазари, настоящи или потенциални клиенти, собственост, методи на работа, персонал, договори, ангажименти, правни въпроси или стратегии, продукти, процеси, свързани с документация, чертежи, спецификации, диаграми, планове, уведомления, данни , образци, модели, мостри, софтуер, софтуерни приложения, компютърни устройства или други материали или записи или друга информация, независимо дали в писмен или устен вид, или съдържаща се на компютърен диск или друго устройство. Не се смята за конфиденциална информацията, касаеща наименованието на договора, стойността и предмета на този договор, с оглед бъдещо позоваване на придобит професионален опит от **ИЗПЪЛНИТЕЛЯ**.

(2) Конфиденциална информация за целите на настоящия договор включва и :

1. съдържанието на данъчна и осигурителна информация, лични данни или друга защитена от закон или по силата на договора информация, която е станала известна при изпълнението на този договор.

2. информация, която е станала известна при изпълнението на този договор относно вътрешни правила и процедури, структура, начин на функциониране на Националната агенция за приходите (НАП) и **ВЪЗЛОЖИТЕЛЯ**, комуникации, мрежи и информационни системи на НАП и на **ВЪЗЛОЖИТЕЛЯ**, изготвени в хода на изпълнението на документи и/или всякакви други резултати от

изпълнението, разработена в полза на НАП или предоставена им документация или програмен код в явен и изпълним вид във връзка с изпълнението на настоящия договор.

(3) Лични данни се обработват от Страните единствено за целите на изпълнение на договора, при стриктно спазване на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и действащата нормативна уредба.

(4) Не се счита за нарушение на задълженията за неразкриване на Конфиденциална информация, когато:

1. Информацията е станала или става публично достъпна, без нарушаване на този договор от която и да е от страните;

2. Информацията се изисква по силата на закон, приложим спрямо която и да е от страните; или

3. Предоставянето на информацията се изисква от регулаторен или друг компетентен орган и съответната страна е длъжна да изпълни такова изискване;

В случаите по точки 2 или 3 страната, която следва да предостави информацията, уведомява незабавно другата страна по договора.

(5) Задълженията на **ИЗПЪЛНИТЕЛЯ** във връзка с изискванията за конфиденциалност включват и:

1. задължение да спазва вътрешните правила за достъп и режим на работа до сградите на НАП и на **ВЪЗЛОЖИТЕЛЯ**, когато е приложимо;

2. да спазва всички процедури и изисквания на НАП за работа в информационната инфраструктура на НАП;

3. да пази в поверителност и да не разкрива или разпространява информация за другата Страна, станала му известна при или по повод изпълнението на дейностите, предмет на договора.

4. представляващите **ИЗПЪЛНИТЕЛЯ** и лицата, които имат достъп до системите на НАП е необходимо за предоставят подписани декларации за опазване на информацията по образец, утвърден от НАП при подписване на договора и при необходимост от предоставяне на достъп до системите на НАП.

(6) С изключение на случаите, посочени в ал. 4, конфиденциална информация може да бъде разкривана само след предварително писмено одобрение от другата страна, като това съгласие не може да бъде отказано безпричинно.

(7) Задълженията по опазване от нерегламентиран достъп до конфиденциална информация се отнасят до **ИЗПЪЛНИТЕЛЯ**, всички негови поделения, контролирани от него фирми и организации, всички негови служители и наети от него физически или юридически лица, в това число

подизпълнители, като **ИЗПЪЛНИТЕЛЯТ** отговаря за изпълнението на тези задължения от страна на такива лица.

(8) Всяка от страните се задължава да информира другата при нарушаване на изискванията за опазване на поверителност на информацията по този договор.

(9) Задълженията, свързани с неразкриването на Конфиденциалната информация остават в сила и след прекратяване на договора, на каквото и да е основание.

XIII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл. 34. (1) Освен ако са дефинирани изрично по друг начин в този договор, използваните в него понятия имат значението, дадено им в ЗОП, съответно в легалните дефиниции в Допълнителните разпоредби на ЗОП или, ако няма такива за някои понятия – според значението, което им се придава в основните разпоредби на ЗОП.

(2) При противоречие между различни разпоредби или условия, съдържащи се в договора и Приложенията, се прилагат следните правила:

1. специалните разпоредби имат предимство пред общите разпоредби;

2. разпоредбите на Приложенията имат предимство пред разпоредбите на Договора.

(3) В случаите, когато **ИЗПЪЛНИТЕЛЯТ** е представил Общи условия в офертата си, при възникнало противоречие между тях и клаузите на настоящия договор, с приоритет се прилагат клаузите на договора.

Чл. 35. Настоящият договор може да бъде изменян или допълван от страните при условията на чл. 116 от ЗОП.

Чл. 36. (1) Всички уведомления между Страните във връзка с този Договор се извършват в писмена форма и могат да се предават лично или чрез препоръчано писмо, по куриер, по факс, електронна поща или по телефон, което се потвърждава писмено на следните адреси:

1. За **ВЪЗЛОЖИТЕЛЯ**:

Адрес за кореспонденция: гр. София 1504, ул. „Панайот Волов“ № 2

Факс: 02/ 943 66 07

e-mail: office@is-bg.net;

тел. 02/942 03 40

2. За **ИЗПЪЛНИТЕЛЯ**:

Адрес за кореспонденция: ул. Тинтява 13, 1113 София;

Факс: 02 960 9797;

e-mail: projects@kontrax.bg (по въпроси относно изпълнението на договора); service@kontrax.bg (за заявки в периода на гаранционния срок по договора);

тел.: 02 960 9777.

(2) Страните упълномощават следните представители, които да проследяват и приемат изпълнението на задълженията им по настоящия договор, да осъществяват контрол по цялостното изпълнение на Договора и да подписват предвидените в Договора документи (уведомления, протоколи и др.), както следва:

1. За **ВЪЗЛОЖИТЕЛЯ**:

[redacted] - Ръководител, информационни и комуникационни технологии, Отдел „Комуникации“, e-mail:[redacted] тел. [redacted]

2. За **ИЗПЪЛНИТЕЛЯ**

[redacted] – проектен мениджър - телефон: [redacted], електронна поща: [redacted]

(3) За дата на получаване на уведомлението/заявката се счита:

1. датата на предаването – при лично предаване на уведомлението;

2. датата на пощенското клеймо на обратната разписка – при изпращане по пощата;

3. датата на доставка, отбелязана върху куриерската разписка – при изпращане по куриер;

4. датата, посочена в извлечението от факс устройството– при изпращане по факс;

5. датата на която уведомлението/заявката е постъпила в посочената от ИЗПЪЛНИТЕЛЯ информационна система (e-mail) – при изпращане по електронна поща.

(4) Всяка кореспонденция между Страните ще се счита за валидна, ако е изпратена на посочените по-горе адреси (в т.ч. електронни), чрез посочените по-горе средства за комуникация и на посочените лица по ал. 2. При промяна на посочените адреси, телефони и други данни за контакт, съответната Страна е длъжна да уведоми другата в писмен вид в срок до 3 (три) работни дни от настъпване на промяната. При неизпълнение на това задължение всяко уведомление ще се счита за валидно връчено, ако е изпратено на посочените по-горе адреси, чрез описаните средства за комуникация и на посочените лица за контакт.

(5) При преобразуване без прекратяване, промяна на наименованието, правноорганизационната форма, седалището, адреса на управление, предмета на дейност, срока на съществуване, органите на управление и представителство на **ИЗПЪЛНИТЕЛЯ**, същият се задължава да уведоми **ВЪЗЛОЖИТЕЛЯ** за промяната в срок до 3 (три) дни от вписването ѝ в съответния регистър.

Чл. 37. Всички спорове по този договор ще се уреждат чрез преговори между страните, а при непостигане на съгласие, ще се отнасят за решаване от компетентния съд в Република България.

Чл. 38. За всички неуредени в този договор въпроси се прилагат разпоредбите на действащото законодателство.

[redacted]

Неразделна част от настоящия договор са:

1. Техническа спецификация на **ВЪЗЛОЖИТЕЛЯ** – Приложение № 1.;

1.1. Приложение № 1.7 – Техническа спецификация, относима към обособена позиция № 7 с предмет „Доставка на система за защита от изтичане/загуба на данни от крайните точки и от мрежата“ - Приложение № 1.7 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)*

2. Техническо предложение на **ИЗПЪЛНИТЕЛЯ** – Приложение № 2.7;

3. Ценовото предложение на **ИЗПЪЛНИТЕЛЯ** – Приложение № 3.7.

При подписване на договора, се представиха следните документи:

1. Гаранция за изпълнение на договора;

2. Документи по чл. 112, ал. 1 от ЗОП.

Настоящият договор се състави в 2 (два) еднообразни оригинални екземпляра на български език – 1 (един) за **ВЪЗЛОЖИТЕЛЯ** и 1 (един) за **ИЗПЪЛНИТЕЛЯ**, и се подписа, както следва:

ЗА ВЪЗЛОЖИТЕЛЯ:

[redacted]

Ивайло Филипов

Изпълнителен директор

[redacted]

Камелия Софрониева

Главен счетоводител

ЗА ИЗПЪЛНИТЕЛЯ:

[redacted]

Николай Йорданов

Изпълнителен директор

КОНТРАКС АД

[redacted]

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

ПО ОТКРИТА ПРОЦЕДУРА ЗА ВЪЗЛАГАНЕ НА ОБЩЕСТВЕНА ПОРЪЧКА С ПРЕДМЕТ:

„ДОСТАВКА НА КОМУНИКАЦИОННО ОБОРУДВАНЕ, ХАРДУЕР И СОФТУЕР, НЕОБХОДИМИ ЗА ОБНОВЯВАНЕ НА ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ СИСТЕМИ НА НАЦИОНАЛНА АГЕНЦИЯ ЗА ПРИХОДИТЕ“

I. ПРЕДМЕТ НА ОБЩЕСТВЕНАТА ПОРЪЧКА

1. В предмета на обществената поръчка по обособени позиции №1, № 2, № 3, № 4, № 5, № 6 и № 9 се включват следните дейности:

1.1. доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция по приходите (наричано по-нататък за краткост „оборудването“), подробно описани по вид, количество и технически характеристики в настоящата Техническата спецификация, Приложенията към нея и Техническото предложение на участника, избран за изпълнител по съответната обособена позиция.

1.2. гаранционно обслужване на доставеното по т. 1.1. оборудване, осигурено в рамките на срока на гаранционно обслужване в съответствие с предписанията на производителя, изискванията на договора за обществена поръчка и приложенията към него.

2. В предмета на обществената поръчка по обособени позиции № 7 и № 8 се включват следните дейности:

2.1. доставка на софтуер, необходим за обновяване на информационни и комуникационни системи на Национална агенция по приходите (наричано по-нататък за краткост „софтуер“ или „доставките“), подробно описан по вид, количество и технически характеристики в настоящата Техническа спецификация, Приложенията към нея и Техническото предложение на участника, избран за изпълнител по съответната обособена позиция.

2.2. гаранционно обслужване на доставения софтуер по т. 2.1 (наричано алтернативно „гаранция и поддръжка“), осигурено в рамките на срока на гаранционно обслужване в съответствие с предписанията на производителя, изискванията на договора за обществена поръчка и приложенията към него.

II. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО НА ПОРЪЧКАТА

1. Навсякъде в техническата спецификация, където се съдържа посочване на конкретен модел, източник, процес, търговска марка, патент, тип, произход, стандарт или производство да се чете и разбира „или ЕКВИВАЛЕНТ".

Важно! *Участникът следва да докаже, че предлаганите решения удовлетворяват по еквивалентен начин изискванията, определени от техническата спецификация.*

2. Оборудването, предмет на доставката, се състои от хардуер и софтуер, които трябва да съответстват или да надвишават в техническо отношение посочените минимални изисквания в настоящата Техническа спецификация и/или приложенията към нея. За целта участникът представя към Техническото си предложение по съответната обособена позиция подробно описание на предлаганото от него оборудване/предлагания софтуер.

3. Оборудването (хардуер и софтуер), предмет на доставката, трябва да бъде фабрично ново, неупотребявано, да е в актуалните продуктови листи на производителя към датата на сключване на договора за възлагане на обществената поръчка и да не е спряно от производство.

4. Хардуерните компоненти на оборудването трябва да отговарят на всички стандарти в Република България относно ергономичност, пожарна безопасност, норми за безопасност и включване към електрическата мрежа.

5. Оборудването следва да бъде доставено в пълно работно състояние, в оригиналната опаковка на производителя с ненарушена цялост, окомплектовано с всички необходими интерфейсни и захранващи кабели, в случай, че са различни от стандартни IEC C14 - IEC C13 или IEC C20 - IEC C19. Необходимата техническа документация, като потребителски, инсталационни, конфигурационни и др. ръководства да се представят на електронен носител за всеки тип от предлаганите устройства.

6. При доставката на софтуер следва да бъдат предоставени необходимите сертификати или други документи, удостоверяващи предоставеното право на ползване на софтуера.

III. УСЛОВИЯ НА ДОСТАВКА

1. Доставката на оборудването (хардуер и софтуер) се извършва въз основа на писмена заявка, отправена чрез адреса за кореспонденция на хартиен носител или по електронна поща, подписана с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис на възложителя или упълномощен негов представител, съгласно клаузите на договора за обществена поръчка. В писмената заявка се посочват:

1.1. Вид и количество на оборудването (хардуер и софтуер), което следва да бъде доставено;

1.2. Място на доставка на оборудването (хардуер и софтуер);

1.3. Срок на доставка, съобразен със сроковете и условията на доставка по договора за обществена поръчка.

1.4. Друга информация по преценка на възложителя, относима към изпълнението на договора за обществена поръчка.

2. Приемането и предаването на изпълнението се осъществява въз основа на изискванията на договора за обществена поръчка.

IV. ГАРАНЦИЯ И ПОДДРЪЖКА. УСЛОВИЯ НА ГАРАНЦИОННО ОБСЛУЖВАНЕ

1. Участникът, избран за изпълнител, гарантира за срока, посочен в т. V.2., пълната функционална годност на доставеното оборудване/доставения софтуер съгласно предписанията на производителя, изискванията на договора за обществена поръчка по съответната обособена позиция и приложенията към него.

2. В рамките на срока по посочен в т. V.2. и в съответствие с режима на гаранционно обслужване участникът, избран за изпълнител, отстранява за своя сметка всички повреди и/или несъответствия на оборудването, съответно подменя дефектирали части, устройства, модули и/или компоненти с нови съгласно предписанията на производителя, изискванията на договора за обществена поръчка по съответната обособена позиция и приложенията към него. В гаранционното обслужване се включва замяна на част (компонент) със скрити недостатъци с нова или на цялото устройство с ново, ако недостатъкът го прави негодно за използване по предназначението му, както и всички разходи по замяната.

3. Режимът на гаранционното обслужване на хардуера е 5 дни в седмицата (от понеделник до петък), 8 часа в рамките на работното време от 9.00 ч. до 17.30 ч.

4. Времето за реакция на избрания за изпълнител участник е до следващия работен ден от уведомяването му.

** Време за реакция е времето от момента на уведомяване от страна на Възложителя за възникнал проблем до обратна реакция (обаждане или пристигане на място) от участника, избран за изпълнител.*

5. Избраният за изпълнител участник е длъжен да осигури преглед на място в срок не по-късно от следващия работен ден от 9.00 ч. до 17.30 ч.

6. Избраният за изпълнител участник се задължава да отстрани настъпилата повреда и/или несъответствие и възстановяване на пълната работоспособност на оборудването. Отстраняването на настъпила повреда и/или несъответствието се осъществява по местоположение на оборудването.

7. При невъзможност за отстраняване на настъпила повреда и/или несъответствие в срок от следващите два работни дни, следва да бъде осигурено оборотно оборудване, притежаващо

характеристиките в Техническото предложение на участника, избран за изпълнител, включително нови алтернативни решения при запазване на пълната изисквана функционалност, до пълното отстраняване на повреда или несъответствие, като срока на гаранционно обслужване на оборудването в процес на поправяне, се удължава със срока, през който е траело отстраняването на повредата.

8. В случай, че повредата и/или несъответствието прави устройството негодно за използване по предназначението му, избраният за изпълнител участник е длъжен да го замени с ново, с параметри гарантиращи същата или по-добра функционалност и производителност.

9. За всяка извършена дейност, избраният за изпълнител участник изготвя и предоставя протокол, който съдържа описание на извършеното. Протоколът се подписва от представители на двете страни.

10.Избраният за изпълнител участник следва да предоставя обобщен отчет за извършените дейности по гаранционно обслужване на всяко тримесечие, които се приемат от възложителя. В обобщените отчети се посочва най-малко следната информация: период на покритие на отчета и списък с възникналите проблеми и параметрите, при които избраният за изпълнител участник е отстранил проблемите.

11.Всички разходи по време на гаранционното обслужване да са за сметка на избрания за изпълнител участник.

V. СРОК НА ИЗПЪЛНЕНИЕ

1. Участникът следва да предложи в офертата си срок за извършване на доставката, който не може да бъде по-дълъг от 80 календарни дни, считано от получаване на писмената заявка по т. III.1.

2. Срокът на гаранционно обслужване е минимум 5 (пет) години, считано от датата на приемо-предавателния протокол за доставка на оборудването (хардуер и софтуер). Участникът следва да посочи в офертата си срок на гаранционно обслужване, който да отговаря на съответните изисквания.

VI. МЯСТО НА ИЗПЪЛНЕНИЕ

1. Мястото на извършване на доставката е на територията на гр. София, като конкретния адрес на извършване на доставката ще бъде посочен в писмената заявка по т. III.1. .

2. Гаранционното обслужване ще се извършва спрямо местонахождението на доставеното и инсталирано оборудване.

VII. ДРУГИ ИЗИСКВАНИЯ. ДОКУМЕНТИ КЪМ ОФЕРТАТА НА УЧАСТНИКА

1. В случай, че не е производител участникът следва да е упълномощен от производителя или от официален представител на производителя за доставка и гаранционно обслужване на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на територията на Република България.

За удостоверяване на горното участникът следва да представи Официално оторизационно писмо (или еквивалентен документ) с актуална дата от производителя или от официален представител на производителя на предлаганото оборудване. Горепосоченият документ се представя в техническото предложение на участника.

Забележка: *В случаите на представяне от участника на оторизационно писмо от официален представител на производителя, в офертата се прилага и оторизационно писмо, издадено от производителя (или еквивалентен документ), с което се упълномощава официалния представител на производителя за доставка и гаранционно обслужване на предлаганото оборудване.*

2. Участникът следва да представи Общи условия или други приложими условия за гаранционно обслужване от производителя на продуктите, предмет на обществената поръчка, като ги приложи към техническото си предложение по съответната обособена позиция, в случай, че е приложимо.

VIII. ПРИЛОЖЕНИЯ:

1. Техническа спецификация по обособена позиция № 1 с предмет: **„Доставка на централен процесорен блок за обработка на информация, софтуерни пакети и операционни системи за виртуализация и сървъри за точно време "** – Приложение № 1.1.;

2. Техническа спецификация по обособена позиция № 2 с предмет: **„Доставка на софтуерно дефинирана мрежа за пренос на данни"** – Приложение № 1.2.;

3. Техническа спецификация по обособена позиция № 3 с предмет: **„Доставка на система за филтриране, проследяване и блокиране на Интернет трафик, система за управление на технически уязвимости и защитни стени за граничен слой"** – Приложение № 1.3.;

4. Техническа спецификация по обособена позиция № 4 с предмет: **„Доставка на дискови масиви за данни и хардуерни устройства и софтуерни пакети за създаване на резервни копия и възстановяване на данни"** – Приложение № 1.4.;

5. Техническа спецификация по обособена позиция № 5 с предмет: **„Доставка на софтуерни пакети и хардуерни устройства за дефиниране на опорна мрежа, мрежово оборудване за достъп до масивите за данни, защитни стени за интернет трафик и електронна поща и за локална мрежа"** – Приложение № 1.5.";

6. Техническа спецификация по обособена позиция № 6 с предмет **„Доставка на хардуерни устройства и софтуерни пакети за платформа за защита от съществуващи и новооткрити кибер заплахи“** – Приложение № 1.6.

7. Техническа спецификация по обособена позиция № 7 с предмет: **„Доставка на система за защита от изтичане/загуба на данни от крайните точки и от мрежата“** – Приложение № 1.7.;

8. Техническа спецификация по обособена позиция № 8 с предмет: **„Доставка на система за управление и контрол на електронната идентичност и достъпа до информацията“** – Приложение № 1.8.;

9. Техническа спецификация по обособена позиция № 9 с предмет: **„Доставка на хардуерни устройства и софтуерни пакети за платформа за управление на събития и сигурността на информацията“** – Приложение № 1.9.

Приложение №1.7

Техническа спецификация по обособена позиция № 7

„Доставка на система за защита от изтичане/загуба на данни от крайните точки и от мрежата“

1. Платформа за защита от изтичане/загуба на данни от крайните точки и от мрежата

Общи изисквания	
REQ.1.	Тип лиценз: абонамент (subscription), с включени 60 месеца поддръжка от производител
REQ.2.	Брой лицензи: 8000
REQ.3.	Решението трябва да разполага с единна централизирана конзола (уеб-базирана конзола, достъпна през уеб браузър, без да изисква инсталирането на допълнителен софтуер), от която да могат да се управляват всички компоненти на DLP: за засичане и спиране на изтичане на данни на мрежово ниво и чрез електронни съобщения (мрежово DLP); за засичане и спиране на изтичане на данни на ниво крайна точка (Endpoint DLP); за откриване и класифициране на данни (Discover).
REQ.4.	Решението да позволява централизирано управление и конфигуриране на политиките за всички продукти (за наблюдение и за превенция, на мрежово ниво и на ниво крайна точка) през уеб-базираната конзола за управление, използвайки еднаква логика за изграждането на политиките им.
REQ.5.	Откъм скалируемост, решението трябва да поддържа надграждане в бъдеще, което да включва управлението на решения за уеб защита и защита на електронна поща, както и на решения за защита на облачни приложения.
REQ.6.	Решението да поддържа интеграция със следните облачни среди: Office365, OneDrive, Box.
REQ.7.	Решението трябва да позволява разполагане на агенти по крайните точки, за засичане и спиране на изтичане на данни на ниво крайна точка, директно от централизираната конзола за управление, използвайки софтуерни методи като GPO, SCCM или други.
REQ.8.	Решението трябва да предоставя информация в централизираната конзола за състоянието на имплементираните агенти по крайните точки, като да информира ако даден агент не функционира правилно.
REQ.9.	Решението да поддържа имплементация на компонентите в Hyper-V или VMware среда.
REQ.10.	Да могат да се създават потребителски акаунти за достъп до решението, като да могат да им се задават различни права за достъп (например даден потребител само да може да преглежда инциденти от конкретни системи, но не и да извършва действия с тях). Да се поддържа ролево-базирана администрация.
REQ.11.	Решението да може да се интегрира с активна директория и да поддържа двуфакторна автентикация.
REQ.12.	Всички компоненти на решението да могат да се конфигурират и обновяват директно от централизираната конзола за управление.

REQ.13.	Решението да може да се интегрира със скачено хранилище за данни (SAN), което да позволява дълготрайно съхранение на събраните сурови данни и метаданни, за покриване на изисквания от различни регулации.
REQ.14.	Решението трябва да предоставя общ графичен изглед в централизираната конзола за управление, които да показва всички инциденти с данни, разделени по степен на риск, тип събития и т.н. Инцидентите да могат да се разследват директно от конзолата за управление.
REQ.15.	Решението да позволява ескалирането на инциденти от критична важност за организацията към определени екипи или отговорни лица, директно от централизираната конзола за управление.
REQ.16.	Всички дейности, свързани с работата на администраторите с възникналите инциденти, да се отчитат и да са видими в централизираната конзола за управление.
REQ.17.	Решението трябва да позволява извличането на файловете с логираните данни за работата му в различни формати, за допълнителен одит. Файловете с логирани данни да са защитени от неправомерно подменяне на информация.
REQ.18.	Решението трябва да може да търси класифицирани данни (Discover) по зададени критерии, като трябва да се запомнят откритите досега данни и при последващо сканиране да се търсят само нови данни, които не са индексирани.
REQ.19.	Решението да може да поставя пръстови отпечатъци (fingerprint) на засечени файлове с класифицирани данни. Хеш сумите на отпечатъците да се съхраняват в база от данни и да могат да се използват за търсене и за изграждане на политики за сигурност.
REQ.20.	Решението да може да използва единна политика за сканиране на данни, независимо от това къде се намират (data-at-rest), къде се трансферират (data-in-motion) или как се използват (data-in-use), както на мрежово ниво, така и на ниво крайна точка. Системата автоматично да може да предприема съответни действия, според засечената заплаха от изтичане на данни.
REQ.21.	Решението да позволява поставянето на оценка на риска от даден инцидент, според количеството класифицирани данни, с които се работи неправомерно, базирайки се на политиките на организацията.
REQ.22.	Решението да разполага с предварително зададени политики, за засичане на неправомерни действия с класифицирани данни, които да отговарят на изискванията на различни регламенти за обработка на данни. Предварително зададените политики да са по категории, според регион и тип индустрия.
REQ.23.	Решението да разполага с предварително зададени политики, които да индикират за неправомерни действия с данни от потребителите на организацията, водещи до риск от изтичане на данните.
REQ.24.	Да се предоставят поне 1500 предварително зададени политики, за да не е необходимо отделянето на много време от администраторите в създаване на собствени политики.
REQ.25.	Решението трябва да позволява задаването на изключения в политиките, за да може да се изключат дадени обекти от сканиране и блокиране и за да се сведат грешните показания до минимум. Да може да се избира на кои приложения им се има доверие да достъпват данни.
REQ.26.	Решението трябва да позволява задаване в политиките за сигурност на държави, към които винаги да е забранен износа на данни по мрежата, освен ако не са конфигурирани изключения.

REQ.27.	Създаването и управлението на политиките трябва да става лесно, през графичния интерфейс за централизирано управление на решението, без да е необходимо използването на сложни скриптове.
REQ.28.	Решението трябва да позволява лесно да се изграждат правилата в политиките за сигурност, като да могат да се използват ключови думи или регулярни изрази (regular expressions), използвайки стандартна булева логика.
REQ.29.	Решението да може да извлича и инспектира текстовото съдържание от файлове и от прикачени файлове в електронни съобщения. Да се предостави пълен списък на поддържаните файлови типове.
REQ.30.	Решението да може да обработва съдържание на кирилица.
REQ.31.	Решението да може да сканира съдържанието на архиви (ZIP, TAR, RAR файлови формати), на до 16 нива навътре при вложени архиви, като да може да засича наличието на класирана информация в тях.
REQ.32.	Решението да може да обработва много големи файлове (от 20MB нагоре) при сканирането за класифицирани данни.
REQ.33.	Решението да може да засича множество случаи на изтичане на данни във времето, породени от един и същ потребител, като да може да създаде общ инцидент при достигане на определено, зададено количество събития. По този начин решението трябва да може да засича опити за частично изнасяне на информация от дадени потребители за дълъг период от време.
REQ.34.	Решението да може да засича изтичане на данни от структурирани системи, което включва бази данни от типа Microsoft SQL Server, Oracle, IBM DB2, както и да всички други типове бази данни, можещи да използват ODBC или OLE конектори за свързване с трети системи.
REQ.35.	Решението да може да прави разлика между различни типове PII или PHI числа при засичането на класифицирани данни. Например, решението да може да прави разлика между деветцифрен номер за социално осигуряване от деветцифрен телефонен номер, без да е необходимо пред числото да има ключова дума, под формата на текст, който да го обособява (например текста „тел. номер“).
REQ.36.	Решението да разполага с machine-learning технология (да използва алгоритми и техники, за да може автоматично да се учи от предишни инциденти)
REQ.37.	Решението да може да използва бели списъци със зададено текстово съдържание, което да се игнорира при сканирането за заплахи.
REQ.38.	Решението да може да сканира за мрежови заплахи за данните в Microsoft Exchange 2013 среда и да може да ги предотвратява.
REQ.39.	Решението да може да работи с класифицирани данни, съдържани във файловете, съхранени в SharePoint 2013 среди.
REQ.40.	Решението да може да открива класифицирани данни по мрежата за Exchange Online и SharePoint Online (Office 365) среди. Решението да може да се интегрира чрез API интерфейса на Microsoft за Office 365.
REQ.41.	Решението да може да работи с описано съдържание под формата на ключови думи и фрази, както и изрази от типа regular expressions.

REQ.42.	Решението да може да засича и блокира криптиран пренос на данни. Да се опишат какви типове криптирана комуникация се поддържат.
REQ.43.	Решението да може да извлича и обработва съдържанието от графични файлови формати, използвайки OCR технология, като например Abbyy FineReader или Nuance. OCR технологията трябва да е вградена в решението, без да е необходимо закупуването на допълнителни лицензи.
REQ.44.	Решението трябва да може да съхранява информация за засечените данни заедно с прилежащите им метаданни (време и дата на инцидента, потребител предизвикал инцидента, използвани протоколи за пренос на данни и т.н.)
REQ.45.	Решението да може да изпраща автоматични аларми под формата на електронни съобщения.
REQ.46.	Решението да може автоматично да завишава степента на риск на даден инцидент (и съответните аларми) ако той се повтори зададен брой пъти в зададен период от време.
REQ.47.	Решението да може автоматично да известява потребителите или техните ръководители, когато нарушат дадена политика.
REQ.48.	Решението да може да предоставя известие на екрана на работната станция на даден потребител, когато той наруши политика, отнасящата се за работата с класифицирани данни за крайни точки.
REQ.49.	Да могат да се задават автоматични действия от системата по различни параметри, например коя политика е нарушена, степента на риска на инцидента, броя събития, използвания протокол за комуникация и т.н.
REQ.50.	Решението да може автоматично да може да копира файловете в карантина, да криптира файловете (допуска се използването и на third-party инструменти за криптиране) или да трие файловете, които са засечени при неправомерни действия.
REQ.51.	Инцидентите директно да могат да се разследват от централизираната конзола за управление.
REQ.52.	Инцидентите ясно да могат да показват причината и конкретните данни, които са довели до нарушаване на политиката, а не само коя политика е нарушена.
REQ.53.	Решението да дава възможност да се освободят (маркират като грешни показания) група инциденти наведнъж от засечените заплахи, например да се освободят множество електронни съобщения от карантината наведнъж.
REQ.54.	Решението да може да дава информация и да изготвя отчети, които да информират кои инциденти и кои потребители носят най-голям риск за организацията и кои инциденти трябва да се разгледат първи, с по-голям приоритет.
REQ.55.	Отчетите да могат да се извличат от системата в различни файлови формати, например PDF и CSV.
REQ.56.	Дадени потребители или група от потребители да могат да се абонират за автоматично получаване на дадени отчети от системата, които да се изпращат по email. Да може да се зададе график (дневно, седмично, месечно и т.н.)
REQ.57.	Всички отчети да са видими и да могат да се управляват от централизираната конзола за управление.

REQ.58.	Решението да разполага с множество отчети по подразбиране (out-of-box), които да покриват най-често срещаните потребности.
REQ.59.	Решението трябва да позволява на администраторите създаването на собствени отчети.
REQ.60.	Решението да може да сканира и блокира (или друго зададено автоматично действие) изходящ уеб трафик, който нарушава политиките за сигурност.
REQ.61.	Решението да може да сканира уеб-трафик за заплахи, включително уеб-базирана поща, уеб-публикации, други протоколи, които използват HTTP и HTTPS, включително прикачени файлове.
REQ.62.	Решението да може да наблюдава и предотвратява опити за уеб-принтиране на класифицирана информация.
REQ.63.	Решението да предоставя детайлна информация за уеб-страниците (не само IP адрес), към които е направен опит за изнасяне на класифицирана информация, включително информация за географското им разположение, като параметрите да могат да бъдат използвани за финна настройка на политиките за сигурност.
REQ.64.	Решението по подразбиране да може да инспектира криптирана SSL комуникация, без тази функция да изисква закупуването на допълнителни модули или да е зависима от използването на ICAP протокол.
REQ.65.	Решението да може да наблюдава уеб-трафика, породен от приложения за комуникация на потребителите (instant messaging), дори когато този трафик преминава по порт 80.
REQ.66.	Решението трябва да може да сканира и блокира (или друго зададено автоматично действие): чувтствителни данни в SMTP трафик, прикачена чувствителна информация към уеб трафик, пренос на чуствителни данни от файлов сървър към работна станция (LAN трафик), пренос на чувствителна информация в PDF формат.
REQ.67.	Решението да може да сканира и блокира (или друго зададено автоматично действие) изходящи електронни email съобщения, които нарушават политиките за сигурност.
REQ.68.	Решението да може да наблюдава и налага политики на email трафика, явяващ се вътрешен за организацията (между служители), включително да се сканират прикачените файлове в съобщенията. Да има интеграция с Microsoft Outlook и IBM Lotus Notes.
REQ.69.	Решението да може да поставя в карантина електронните съобщения, които нарушават политиките за сигурност на класифицираните данни на организацията. Да има възможност за ръчно освобождаване на електронни съобщения от карантината.
REQ.70.	Решението да може да анализира трафика, преминаващ през Mail Transfer Agent (MTA)
REQ.71.	Решението да може да засича и блокира (или друго зададено автоматично действие) опити на потребители за копиране на класифицирани данни на преносими устройства (например USB устройства, флопи дискове, CD/DVD, т.н.). Да може да се блокира преноса на данни, независимо дали потребителската крайна точка се намира в или извън мрежата на организацията.
REQ.72.	Решението да може да засича и блокира (или друго зададено автоматично действие) опити на потребители или на приложения да извличат класифицирани данни чрез clipboard, print screen команди и други сходни методи.
REQ.73.	Агента за защита на крайните точки да поддържа работа с крайни точки като Windows Server 2016 и Windows 10 (1709, 1803, 1809, 1903), както и с MacOS.

REQ.74.	Решението да може да се интегрира напълно с трети решения като Titus, Boldon James или Microsoft Azure Information Protection, с цел поставяне на етикети на класифицираните данни.
REQ.75.	Решението за защита от изтичане на данни от крайните точки да може да обработвка класифицирана информация, дори когато крайната точка се намира извън мрежата на организацията.
REQ.76.	Решението да позволява налагането на политики за сигурност на структурирани и на неструктурирани данни, дори когато крайната точка се намира извън мрежата на организацията.
REQ.77.	Решението за защита от изтичане на данни от крайните точки да позволява създаването на bypass пароли, които да позволяват локално или отдалечено временно да се спира работата на агента за сигурност на решението (да не се анализират или блократ действия временно на дадената крайна точка).
REQ.78.	Решението за защита от изтичане на данни от крайните точки да позволява извеждането на диалогов прозорец на крайните точки при дадени действия, който да очаква отговор от потребителите с обосноваване на причините за действието с класифицирани данни.
Гаранция и поддръжка:	
REQ.79.	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.80.	Получаване на нови версии на софтуера - 5 (пет) години.

ПРИЛОЖЕНИЕ № 2.7

ДО
„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД
ГР. СОФИЯ, УЛИЦА „ПАНАЙОТ ВОЛОВ“ № 2

ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ

Наименование на обществената поръчка:	***„Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите”***
Наименование на обособена позиция, за която участникът подава оферта	***Обособена позиция № 7: „Доставка на система за защита от изтичане/загуба на данни от крайните точки и от мрежата“***
Наименование на участника:	***КОНТРАКС АД***
Правно-организационна форма на участника:	***Акционерно дружество*** *(физическо или юридическо лице, обединение или друго образувание, което има право да изпълнява доставки съгласно законодателството на държавата, в която е установено)*
Седалище по регистрация и адрес на управление:	**Град София, 1113, ул. „Тинтява“ №13**
ЕИК / Код по регистър БУЛСТАТ/ регистрационен номер или друг идентификационен код:	**175415627**
Представляващ	**Николай Йорданов – Изпълнителен директор** *(законен представител или лице, специално упълномощено за участие в процедурата[1])*

УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА,

[1] Съгласно чл. 41, ал. 5 от Правилника за прилагане на Закона за обществените поръчки (ППЗОП) когато документи, свързани с участие в обществени поръчки се подават от лице, което представя участника по пълномощие, в Единния европейски документ за обществени поръчки (ЕЕДОП) се посочва информация относно обхвата на представителната му власт.

Заличаванията на информация в документа са на основание чл. 4 от Общ регламент за защ данните

След запознаване с документацията за участие в обществената поръчка с горепосочения предмет, ние предоставяме следното техническо предложение по горецитираната обособена позиция, съдържащо:

I.ПРЕДЛОЖЕНИЕ ЗА ИЗПЪЛЕНИЕ НА ПОРЪЧКАТА

В качеството си на представляващ участника, декларирам, че сме запознати с условията на поръчката и с подаването на настоящото предложение удостоверявам следното:

1. Предмет на обществената поръчка:

1.1. Декларирам, че представляваният от мен участник ще изпълни поръчката, съобразявайки се с условията по изпълнение, посочени от възложителя в документацията за обществената поръчка.

1.2. Запознати сме, че съгласно чл. 39, ал. 1 от Правилника за прилагане на Закона за обществените поръчки (ППЗОП) с подаването на офертата по настоящата обществена поръчка се счита, че се съгласяваме с всички условия на възложителя, в т.ч. с определения срок за валидност на офертата и с проекта на договор, неразделна част от документацията за обществената поръчка.

1.3. Задължаваме се да извършим следните дейности:

1.3.1. доставка на софтуер, необходим за обновяване на информационни и комуникационни системи на Национална агенция по приходите (наричано по-нататък за краткост „софтуер"), подробно описано по вид, количество и технически характеристики в Техническата спецификация, Приложение 1.7. към нея, относимо към настоящата обособена позиция, за която подаваме оферта и настоящето Техническо предложение.

1.3.2. гаранционно обслужване на доставения по т. 1.3.1. софтуер (наричано по-нататък алтернативно „гаранция и поддръжка"), осигурено в рамките на срока по т. 4.2. в съответствие с предписанията на производителя, изискванията на договора за обществена поръчка и приложенията към него.

1.4. Подробно описание на вида, обема и техническите характеристики на доставения от нас софтуер е описан, както следва:

1.4.1. Платформа за защита от изтичане/загуба на данни от крайните точки и от мрежата

Изискано от Възложителя		**Предложено от участника**
А.		**Б.**
Общи изисквания		
REQ.1.	Тип лиценз: абонамент (subscription), с включени 60 месеца поддръжка от производител	Предлаганата от нас платформа за защита от изтичане/загуба на данни от крайните точки и от

		мрежата включва лицензионен абонамент тип subscriptions **Forcepoint DLP Suite (IP Protection), User & Data Security** за 60 месеца с включена поддръжка от производителя
REQ.2.	Брой лицензи: 8000	Предлаган брой лицензи: 8000
REQ.3.	Решението трябва да разполага с единна централизирана конзола (уеб-базирана конзола, достъпна през уеб браузър, без да изисква инсталирането на допълнителен софтуер), от която да могат да се управляват всички компоненти на DLP: за засичане и спиране на изтичане на данни на мрежово ниво и чрез електронни съобщения (мрежово DLP); за засичане и спиране на изтичане на данни на ниво крайна точка (Endpoint DLP); за откриване и класифициране на данни (Discover).	Решението разполага с единна централизирана конзола (уеб-базирана конзола, достъпна през уеб браузър, без да изисква инсталирането на допълнителен софтуер), от която могат да се управляват всички компоненти на DLP: за засичане и спиране на изтичане на данни на мрежово ниво и чрез електронни съобщения (мрежово DLP); за засичане и спиране на изтичане на данни на ниво крайна точка (Endpoint DLP); за откриване и класифициране на данни (Discover). Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.4.	Решението да позволява централизирано управление и конфигуриране на политиките за всички продукти (за наблюдение и за превенция, на мрежово ниво и на ниво крайна точка) през уеб-базираната конзола за управление, използвайки еднаква логика за изграждането на политиките им.	Решението позволява централизирано управление и конфигуриране на политиките за всички продукти (за наблюдение и за превенция, на мрежово ниво и на ниво крайна точка) през уеб-базираната конзола за управление, използвайки еднаква логика за изграждането на политиките им. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.5.	Откъм скалируемост, решението трябва да поддържа надграждане в бъдеще, което да включва управлението на решения за уеб защита и защита на електронна поща, както и	Откъм скалируемост решението поддържа надграждане в бъдеще, което включва управлението на решения за уеб защита и защит на електронна поща, както и на решения за защит на облачни приложения.

	на решения за защита на облачни приложения.	Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.6.	Решението да поддържа интеграция със следните облачни среди: Office365, OneDrive, Box.	Решението поддържа интеграция със следните облачни среди: Office365, OneDrive, Box. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.7.	Решението трябва да позволява разполагане на агенти по крайните точки, за засичане и спиране на изтичане на данни на ниво крайна точка, директно от централизираната конзола за управление, използвайки софтуерни методи като GPO, SCCM или други.	Решението позволява разполагане на агенти по крайните точки, за засичане и спиране на изтичане на данни на ниво крайна точка, директно от централизираната конзола за управление, използвайки софтуерни методи като GPO, SCCM или други. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.8.	Решението трябва да предоставя информация в централизираната конзола за състоянието на имплементираните агенти по крайните точки, като да информира ако даден агент не функционира правилно.	Решението предоставя информация в централизираната конзола за състоянието на имплементираните агенти по крайните точки, като информира, ако даден агент не функционира правилно. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.9.	Решението да поддържа имплементация на компонентите в Hyper-V или VMware среда.	Решението поддържа имплементация на компонентите в Hyper-V или VMware среда. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf

REQ.10.	Да могат да се създават потребителски акаунти за достъп до решението, като да могат да им се задават различни права за достъп (например даден потребител само да може да преглежда инциденти от конкретни системи, но не и да извършва действия с тях). Да се поддържа ролево-базирана администрация.	Могат да се създават потребителски акаунти за достъп до решението, като могат да им се задават различни права за достъп (например даден потребител само може да преглежда инциденти от конкретни системи, но не може да извършва действия с тях. Поддържа се ролево-базирана администрация. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.11.	Решението да може да се интегрира с активна директория и да поддържа двуфакторна автентикация.	Решението може да се интегрира с активна директория и поддържа двуфакторна автентикация. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.12.	Всички компоненти на решението да могат да се конфигурират и обновяват директно от централизираната конзола за управление.	Всички компоненти на решението могат да се конфигурират и обновяват директно от централизираната конзола за управление. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.13.	Решението да може да се интегрира със скачено хранилище за данни (SAN), което да позволява дълготрайно съхранение на събраните сурови данни и метаданни, за покриване на изисквания от различни регулации.	Решението може да се интегрира със скачено хранилище за данни (SAN), което позволява дълготрайно съхранение на събраните сурови данни и метаданни, за покриване на изисквания от различни регулации. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.14.	Решението трябва да предоставя общ графичен изглед в централизираната конзола	Решението предоставя общ графичен изглед в централизираната конзола за управление, които

	за управление, които да показва всички инциденти с данни, разделени по степен на риск, тип събития и т.н. Инцидентите да могат да се разследват директно от конзолата за управление.	показват всички инциденти с данни, разделени по степен на риск, тип събития и т.н. Инцидентите могат да се разследват директно от конзолата за управление. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.15.	Решението да позволява ескалирането на инциденти от критична важност за организацията към определени екипи или отговорни лица, директно от централизираната конзола за управление.	Решението позволява ескалирането на инциденти от критична важност за организацията към определени екипи или отговорни лица, директно от централизираната конзола за управление. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.16.	Всички дейности, свързани с работата на администраторите с възникналите инциденти, да се отчитат и да са видими в централизираната конзола за управление.	Всички дейности, свързани с работата на администраторите с възникналите инциденти, се отчитат и са видими в централизираната конзола за управление. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.17.	Решението трябва да позволява извличането на файловете с логираните данни за работата му в различни формати, за допълнителен одит. Файловете с логирани данни да са защитени от неправомерно подменяне на информация.	Решението позволява извличането на файловете с логираните данни за работата му в различни формати, за допълнителен одит. Файловете с логирани данни са защитени от неправомерно подменяне на информация. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.18.	Решението трябва да може да търси класифицирани данни (Discover) по зададени критерии, като трябва да се запомнят	Решението може да търси класифицирани данни (Discover) по зададени критерии, като се запомнят откритите досега данни и при последващо

	открытите досега данни и при последващо сканиране да се търсят само нови данни, които не са индексирани.	сканиране се търсят само нови данни, които не са индексирани. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.19.	Решението да може да поставя пръстови отпечатъци (fingerprint) на засечени файлове с класифицирани данни. Хеш сумите на отпечатъците да се съхраняват в база от данни и да могат да се използват за търсене и за изграждане на политики за сигурност.	Решението може да поставя пръстови отпечатъци (fingerprint) на засечени файлове с класифицирани данни. Хеш сумите на отпечатъците се съхраняват в база от данни и могат да се използват за търсене и за изграждане на политики за сигурност. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.20.	Решението да може да използва единна политика за сканиране на данни, независимо от това къде се намират (data-at-rest), къде се трансферират (data-in-motion) или как се използват (data-in-use), както на мрежово ниво, така и на ниво крайна точка. Системата автоматично да може да предприема съответни действия, според засечената заплаха от изтичане на данни.	Решението може да използва единна политика за сканиране на данни, независимо от това, къде се намират (data-at-rest), къде се трансферират (data-in-motion) или как се използват (data-in-use), както на мрежово ниво, така и на ниво крайна точка. Системата автоматично може да предприема съответни действия, според засечената заплаха от изтичане на данни. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.21.	Решението да позволява поставянето на оценка на риска от даден инцидент, според количеството класифицирани данни, с които се работи неправомерно, базирайки се на политиките на организацията.	Решението позволява поставянето на оценка на риска от даден инцидент, според количеството класифицирани данни, с които се работи неправомерно, базирайки се на политиките на организацията. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.22.	Решението да разполага с предварително зададени политики, за засичане на неправомерни действия с класифицирани	Решението разполага с предварително зададени политики, за засичане на неправомерни действия с класифицирани данни, които отговарят на

	данни, които да отговарят на изискванията на различни регламенти за обработка на данни. Предварително зададените политики да са по категории, според регион и тип индустрия.	изискванията на различни регламенти за обработка на данни. Предварително зададените политики са по категории, според регион и тип индустрия. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.23.	Решението да разполага с предварително зададени политики, които да индикират за неправомерни действия с данни от потребителите на организацията, водещи до риск от изтичане на данните.	Решението разполага с предварително зададени политики, които индикират за неправомерни действия с данни от потребителите на организацията, водещи до риск от изтичане на данните. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.24.	Да се предоставят поне 1500 предварително зададени политики, за да не е необходимо отделянето на много време от администраторите в създаване на собствени политики.	Предоставят се 1800 предварително зададени политики, по този начин не е необходимо отделянето на много време от администраторите в създаване на собствени политики. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.25.	Решението трябва да позволява задаването на изключения в политиките, за да може да се изключат дадени обекти от сканиране и блокиране и за да се сведат грешните показания до минимум. Да може да се избира на кои приложения им се има доверие да достъпват данни.	Решението позволява задаването на изключения в политиките, като по този начин може да се изключат дадени обекти от сканиране и блокиране и грешните показания се свеждат до минимум. Може да се избира на кои приложения, може да им се има доверие да достъпват данни. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.26.	Решението трябва да позволява задаване в политиките за сигурност на държави, към които винаги да е забранен износа на данни по	Решението позволява задаване в политиките за сигурност на държави, към които винаги да е забранен износа на данни по мрежата, освен ако не са конфигурирани изключения.

	мрежата, освен ако не са конфигурирани изключения.	Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.27.	Създаването и управлението на политиките трябва да става лесно, през графичния интерфейс за централизирано управление на решението, без да е необходимо използването на сложни скриптове.	Създаването и управлението на политиките става лесно, през графичния интерфейс за централизирано управление на решението, без да е необходимо използването на сложни скриптове. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.28.	Решението трябва да позволява лесно да се изграждат правилата в политиките за сигурност, като да могат да се използват ключови думи или регулярни изрази (regular expressions), използвайки стандартна булева логика.	Решението позволява лесно да се изграждат правилата в политиките за сигурност, като могат да се използват ключови думи или регулярни изрази (regular expressions), използвайки стандартна булева логика. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.29.	Решението да може да извлича и инспектира текстовото съдържание от файлове и от прикачени файлове в електронни съобщения. Да се предостави пълен списък на поддържаните файлови типове.	Решението може да извлича и инспектира текстовото съдържание от файлове и от прикачени файлове в електронни съобщения. Предоставя се пълен списък на поддържаните файлови типове. Пълен списък на поддържаните файлови типове ще намерите на следния адрес: https://www.websense.com/content/support/library/data/v871/file_support/file_formats.aspx
REQ.30.	Решението да може да обработва съдържание на кирилица.	Решението може да обработва съдържание на кирилица. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.31.	Решението да може да сканира съдържанието на архиви (ZIP, TAR, RAR файлови формати), на до 16 нива навътре при вложени архиви, като да може да засича наличието на класирана информация в тях.	Решението може да сканира съдържанието на архиви (ZIP, TAR, RAR файлови формати), на до 16 нива навътре при вложени архиви, като може да засича наличието на класифицирана информация в тях. Източник:

		https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.32.	Решението да може да обработва много големи файлове (от 20MB нагоре) при сканирането за класифицирани данни.	Решението може да обработва много големи файлове (от 20MB нагоре) при сканирането за класифицирани данни. Максималната големина може да се задава, по подразбиране е определена като 50MB от най-добри практики. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.33.	Решението да може да засича множество случаи на изтичане на данни във времето, породени от един и същ потребител, като да може да създаде общ инцидент при достигане на определено, зададено количество събития. По този начин решението трябва да може да засича опити за частично изнасяне на информация от дадени потребители за дълъг период от време.	Решението може да засича множество случаи на изтичане на данни във времето, породени от един и същ потребител, като може да създаде общ инцидент при достигане на определено, зададено количество събития. По този начин решението може да засича опити за частично изнасяне на информация от дадени потребители за дълъг период от време. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.34.	Решението да може да засича изтичане на данни от структурирани системи, което включва бази данни от типа Microsoft SQL Server, Oracle, IBM DB2, както и да всички други типове бази данни, можещи да използват ODBC или OLE конектори за свързване с трети системи.	Решението може да засича изтичане на данни от структурирани системи, което включва бази данни от типа Microsoft SQL Server, Oracle, IBM DB2, както и всички други типове бази данни, можещи да използват ODBC или OLE конектори за свързване с трети системи. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.35.	Решението да може да прави разлика между различни типове PII или PHI числа при засичането на класифицирани данни. Например, решението да може да прави разлика между деветцифрен номер за	Решението може да прави разлика между различни типове PII или PHI числа при засичането на класифицирани данни. Например, решението може да прави разлика между деветцифрен номер за социално осигуряване от деветцифрен

	социално осигуряване от деветцифрен телефонен номер, без да е необходимо пред числото да има ключова дума, под формата на текст, който да го обособява (например текста „тел. номер“).	телефонен номер, без да е необходимо пред числото да има ключова дума, под формата на текст, който да го обособява (например текста „тел. номер“). Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.36.	Решението да разполага с machine-learning технология (да използва алгоритми и техники, за да може автоматично да се учи от предишни инциденти)	Решението разполага с machine-learning технология (използва алгоритми и техники, за да може автоматично да се учи от предишни инциденти) Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.37.	Решението да може да използва бели списъци със зададено текстово съдържание, което да се игнорира при сканирането за заплахи.	Решението може да използва бели списъци със зададено текстово съдържание, което се игнорира при сканирането за заплахи. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.38.	Решението да може да сканира за мрежови заплахи за данните в Microsoft Exchange 2013 среда и да може да ги предотвратява.	Решението може да сканира за мрежови заплахи за данните в Microsoft Exchange 2013 среда и може да ги предотвратява. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.39.	Решението да може да работи с класифицирани данни, съдържани във файловете, съхранени в SharePoint 2013 среди.	Решението може да работи с класифицирани данни, съдържани във файловете, съхранени в SharePoint 2013 среди. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.40.	Решението да може да открива класифицирани данни по мрежата за Exchange Online и SharePoint Online (Office	Решението може да открива класифицирани данни по мрежата за Exchange Online и SharePoint Online (Office 365) среди. Решението може да се

	365) среди. Решението да може да се интегрира чрез API интерфейса на Microsoft за Office 365.	интегрира чрез API интерфейса на Microsoft за Office 365. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.41.	Решението да може да работи с описано съдържание под формата на ключови думи и фрази, както и изрази от типа regular expressions.	Решението може да работи с описано съдържание под формата на ключови думи и фрази, както и изрази от типа regular expressions. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.42.	Решението да може да засича и блокира криптиран пренос на данни. Да се опишат какви типове криптирана комуникация се поддържат.	Решението може да засича и блокира криптиран пренос на данни. Поддържат се следните типове криптирана комуникация (но е лимитарно само до): • защитени с парола файлове • HTTP през SSL • криптирани Excel файлове • криптирани PDF документи • PGP компресирани данни • PGP криптирани данни • набор от PGP публични ключове • набор от PGP тайни ключове • PGP сертификат за подпис • PGP подписани данни • PGP подписани и криптирани данни • криптирани MS Word документи • криптирани архиви като ZIP и ARC Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.43.	Решението да може да извлича и обработва съдържанието от графични файлови формати, използвайки OCR технология, като например Abbyy FineReader или Nuance. OCR	Решението може да извлича и обработва съдържанието от графични файлови формати, използвайки OCR технология, като например Abbyy FineReader или Nuance. OCR технологията е

	технологията трябва да е вградена в решението, без да е необходимо закупуването на допълнителни лицензи.	вградена в решението, без да е необходимо закупуването на допълнителни лицензи. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.44.	Решението трябва да може да съхранява информация за засечените данни заедно с прилежащите им метаданни (време и дата на инцидента, потребител предизвикал инцидента, използвани протоколи за пренос на данни и т.н.)	Решението може да съхранява информация за засечените данни заедно с прилежащите им метаданни (време и дата на инцидента, потребител предизвикал инцидента, използвани протоколи за пренос на данни и т.н.) Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.45.	Решението да може да изпраща автоматични аларми под формата на електронни съобщения.	Решението може да изпраща автоматични аларми под формата на електронни съобщения. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.46.	Решението да може автоматично да завишава степента на риск на даден инцидент (и съответните аларми) ако той се повтори зададен брой пъти в зададен период от време.	Решението може автоматично да завишава степента на риск на даден инцидент (и съответните аларми), ако той се повтори зададен брой пъти в зададен период от време. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.47.	Решението да може автоматично да известява потребителите или техните ръководители, когато нарушат дадена политика.	Решението може автоматично да известява потребителите или техните ръководители, когато нарушат дадена политика. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.48.	Решението да може да предоставя известие на екрана на работната станция на даден потребител, когато той наруши политика,	Решението може да предоставя известие на екрана на работната станция на даден потребител, когато той наруши политика, отнасящата се за работата с класифицирани данни за крайни точки.

	отнасящата се за работата с класифицирани данни за крайни точки.	Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.49.	Да могат да се задават автоматични действия от системата по различни параметри, например коя политика е нарушена, степента на риска на инцидента, броя събития, използвания протокол за комуникация и т.н.	Могат да се задават автоматични действия от системата по различни параметри, например коя политика е нарушена, степента на риска на инцидента, броя събития, използвания протокол за комуникация и т.н. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.50.	Решението да може автоматично да може да копира файловете в карантина, да криптира файловете (допуска се използването и на third-party инструменти за криптиране) или да трие файловете, които са засечени при неправомерни действия.	Решението може автоматично да може да копира файловете в карантина, криптира файловете (допуска се използването и на third-party инструменти за криптиране) или трие файловете, които са засечени при неправомерни действия. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.51.	Инцидентите директно да могат да се разследват от централизираната конзола за управление.	Инцидентите директно могат да се разследват от централизираната конзола за управление. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.52.	Инцидентите ясно да могат да показват причината и конкретните данни, които са довели до нарушаване на политиката, а не само коя политика е нарушена.	Инцидентите ясно могат да показват причината и конкретните данни, които са довели до нарушаване на политиката, а не само коя политика е нарушена. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.53.	Решението да дава възможност да се освободят (маркират като грешни показания) група инциденти наведнъж от засечените заплахи, например да се освободят	Решението дава възможност да се освободят (маркират като грешни показания) група инциденти наведнъж от засечените заплахи, например освобождават се множество електронни съобщения от карантината наведнъж.

	множество електронни съобщения от карантината наведнъж.	Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.54.	Решението да може да дава информация и да изготвя отчети, които да информират кои инциденти и кои потребители носят най-голям риск за организацията и кои инциденти трябва да се разгледат първи, с по-голям приоритет.	Решението може да дава информация и да изготвя отчети, които да информират кои инциденти и кои потребители носят най-голям риск за организацията и кои инциденти трябва да се разгледат първи, с по-голям приоритет. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.55.	Отчетите да могат да се извличат от системата в различни файлови формати, например PDF и CSV.	Отчетите могат да се извличат от системата в различни файлови формати, например PDF и CSV. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.56.	Дадени потребители или група от потребители да могат да се абонират за автоматично получаване на дадени отчети от системата, които да се изпращат по email. Да може да се зададе график (дневно, седмично, месечно и т.н.)	Дадени потребители или група от потребители могат да се абонират за автоматично получаване на дадени отчети от системата, които се изпращат по email. Може да се зададе график (дневно, седмично, месечно и т.н.) Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.57.	Всички отчети да са видими и да могат да се управляват от централизираната конзола за управление.	Всички отчети са видими и могат да се управляват от централизираната конзола за управление. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.58.	Решението да разполага с множество отчети по подразбиране (out-of-box), които да покриват най-често срещаните потребности.	Решението разполага с множество отчети по подразбиране (out-of-box), които покриват най-често срещаните потребности. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf

REQ.59.	Решението трябва да позволява на администраторите създаването на собствени отчети.	Решението позволява на администраторите създаването на собствени отчети. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.60.	Решението да може да сканира и блокира (или друго зададено автоматично действие) изходящ уеб трафик, който нарушава политиките за сигурност.	Решението може да сканира и блокира (или друго зададено автоматично действие) изходящ уеб трафик, който нарушава политиките за сигурност. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.61.	Решението да може да сканира уеб-трафик за заплахи, включително уеб-базирана поща, уеб-публикации, други протоколи, които използват HTTP и HTTPS, включително прикачени файлове.	Решението може да сканира уеб-трафик за заплахи, включително уеб-базирана поща, уеб-публикации, други протоколи, които използват HTTP и HTTPS, включително прикачени файлове. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.62.	Решението да може да наблюдава и предотвратява опити за уеб-принтиране на класифицирана информация.	Решението може да наблюдава и предотвратява опити за уеб-принтиране на класифицирана информация. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.63.	Решението да предоставя детайлна информация за уеб-страниците (не само IP адрес), към които е направен опит за изнасяне на класифицирана информация, включително информация за географското им разположение, като параметрите да могат да бъдат използвани за финна настройка на политиките за сигурност.	Решението предоставя детайлна информация за уеб-страниците (не само IP адрес), към които е направен опит за изнасяне на класифицирана информация, включително информация за географското им разположение, като параметрите могат да бъдат използвани за финна настройка на политиките за сигурност. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf

REQ.64.	Решението по подразбиране да може да инспектира криптирана SSL комуникация, без тази функция да изисква закупуването на допълнителни модули или да е зависима от използването на ICAP протокол.	Решението по подразбиране може да инспектира криптирана SSL комуникация, като тази функция не изисква закупуването на допълнителни модули или не е зависима от използването на ICAP протокол. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.65.	Решението да може да наблюдава уеб-трафика, породен от приложения за комуникация на потребителите (instant messaging), дори когато този трафик преминава по порт 80.	Решението може да наблюдава уеб-трафика, породен от приложения за комуникация на потребителите (instant messaging), дори когато този трафик преминава по порт 80. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.66.	Решението трябва да може да сканира и блокира (или друго зададено автоматично действие): чувствителни данни в SMTP трафик, прикачена чувствителна информация към уеб трафик, пренос на чувствителни данни от файлов сървър към работна станция (LAN трафик), пренос на чувствителна информация в PDF формат.	Решението може да сканира и блокира (или друго зададено автоматично действие): чувствителни данни в SMTP трафик, прикачена чувствителна информация към уеб трафик, пренос на чувствителни данни от файлов сървър към работна станция (LAN трафик), пренос на чувствителна информация в PDF формат. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.67.	Решението да може да сканира и блокира (или друго зададено автоматично действие) изходящи електронни email съобщения, които нарушават политиките за сигурност.	Решението може да сканира и блокира (или друго зададено автоматично действие) изходящи електронни email съобщения, които нарушават политиките за сигурност. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.68.	Решението да може да наблюдава и налага политики на email трафика, явяващ се вътрешен за организацията (между служители), включително да се сканират	Решението може да наблюдава и налага политики на email трафика, явяващ се вътрешен за организацията (между служители), включително се сканират прикачените файлове в съобщенията.

	прикачените файлове в съобщенията. Да има интеграция с Microsoft Outlook и IBM Lotus Notes.	Има интеграция с Microsoft Outlook и IBM Lotus Notes. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.69.	Решението да може да поставя в карантина електронните съобщения, които нарушават политиките за сигурност на класифицираните данни на организацията. Да има възможност за ръчно освобождаване на електронни съобщения от карантината.	Решението може да поставя в карантина електронните съобщения, които нарушават политиките за сигурност на класифицираните данни на организацията. Има възможност за ръчно освобождаване на електронни съобщения от карантината. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.70.	Решението да може да анализира трафика, преминаващ през Mail Transfer Agent (MTA)	Решението може да анализира трафика, преминаващ през Mail Transfer Agent (MTA) Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.71.	Решението да може да засича и блокира (или друго зададено автоматично действие) опити на потребители за копиране на класифицирани данни на преносими устройства (например USB устройства, флопи дискове, CD/DVD, т.н.). Да може да се блокира преноса на данни, независимо дали потребителската крайна точка се намира в или извън мрежата на организацията.	Решението може да засича и блокира (или друго зададено автоматично действие) опити на потребители за копиране на класифицирани данни на преносими устройства (например USB устройства, флопи дискове, CD/DVD, т.н.). Може да се блокира преносът на данни, независимо дали потребителската крайна точка се намира в или извън мрежата на организацията. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.72.	Решението да може да засича и блокира (или друго зададено автоматично действие) опити на потребители или на приложения да	Решението може да засича и блокира (или друго зададено автоматично действие) опити на потребители или на приложения да извличат класифицирани данни чрез clipboard, print screen команди и други сходни методи.

	извличат класифицирани данни чрез clipboard, print screen команди и други сходни методи.	Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.73.	Агента за защита на крайните точки да поддържа работа с крайни точки като Windows Server 2016 и Windows 10 (1709, 1803, 1809, 1903), както и с MacOS.	Агентът за защита на крайните точки поддържа работа с крайни точки като Windows Server 2016 и Windows 10 (1709, 1803, 1809, 1903), както и с MacOS. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.74.	Решението да може да се интегрира напълно с трети решения като Titus, Boldon James или Microsoft Azure Information Protection, с цел поставяне на етикети на класифицираните данни.	Решението може да се интегрира напълно с трети решения като Titus, Boldon James или Microsoft Azure Information Protection, с цел поставяне на етикети на класифицираните данни. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.75.	Решението за защита от изтичане на данни от крайните точки да може да обработва класифицирана информация, дори когато крайната точка се намира извън мрежата на организацията.	Решението за защита от изтичане на данни от крайните точки може да обработва класифицирана информация, дори когато крайната точка се намира извън мрежата на организацията. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.76.	Решението да позволява налагането на политики за сигурност на структурирани и на неструктурирани данни, дори когато крайната точка се намира извън мрежата на организацията.	Решението позволява налагането на политики за сигурност на структурирани и на неструктурирани данни, дори когато крайната точка се намира извън мрежата на организацията. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.77.	Решението за защита от изтичане на данни от крайните точки да позволява създаването на bypass пароли, които да позволяват локално или отдалечено временно да се спира	Решението за защита от изтичане на данни от крайните точки позволява създаването на bypass пароли, които позволяват локално или отдалечено временно да се спира работата на агента за

	работата на агента за сигурност на решението (да не се анализират или блокират действия временно на дадената крайна точка).	сигурност на решението (не се анализират или блокират действия временно на дадената крайна точка). Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
REQ.78.	Решението за защита от изтичане на данни от крайните точки да позволява извеждането на диалогов прозорец на крайните точки при дадени действия, който да очаква отговор от потребителите с обосноваване на причините за действието с класифицирани данни.	Решението за защита от изтичане на данни от крайните точки позволява извеждането на диалогов прозорец на крайните точки при дадени действия, който очаква отговор от потребителите с обосноваване на причините за действието с класифицирани данни. Източник: https://www.websense.com/content/support/library/data/v87/help/help.pdf https://www.websense.com/content/support/library/data/v871/install/install_dlp.pdf
Гаранция и поддръжка:		**Предлагана гаранция и поддръжка от производителя:**
REQ.79.	Срок на техническа поддръжка – минимум 5 (пет) години.	Срокът на техническата поддръжка е 5 (пет) години.
REQ.80.	Получаване на нови версии на софтуера - минимум 5 (пет) години.	Получаването на новите версии на софтуера е 5 (пет) години.

Забележка: а) *Навсякъде в техническата спецификация, където се съдържа посочване на конкретен модел, източник, процес, търговска марка, патент, тип, произход, стандарт или производство да се чете и разбира „или ЕКВИВАЛЕНТ“. Участникът следва да докаже, че предлаганите решения удовлетворяват по еквивалентен начин изискванията, определени от техническата спецификация.*

б) *Предметът на доставка трябва да съответства или да надвишава в техническо отношение посочените минимални изисквания в Техническата спецификация и приложението към нея, относимо към настоящата обособена позиция.*

2. Условия на доставка

2.1. Запознати сме, че доставката на софтуера ще се извършва въз основа на писмена заявка, отправена чрез адреса за кореспонденция на хартиен носител или по електронна поща, подписана с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис на

възложителя или упълномощен негов представител, съгласно клаузите на договора за обществена поръчка.

2.2. Приемането и предаването на изпълнението ще се осъществява въз основа на изискванията на договора за обществена поръчка.

3. Условия на гаранционно обслужване

3.1. Гарантираме за срока, посочен в т. 4.2., пълната функционална годност на доставения софтуер съгласно предписанията на производителя, изискванията на договора за обществена поръчка по обособената позиция, за която предоставяме настоящето Техническо предложение и приложенията към него.

4. Срок на изпълнение

4.1. Задължаваме се да извършим доставка на софтуера в срок до 10 календарни дни, считано от датата на получаване на писмена заявка по чл. 1, ал. 2 от проекта на договор за обществена поръчка.

***Забележка**: Участникът следва да предложи в офертата си срок за извършване на доставката, който не може да бъде по-дълъг от 80 календарни дни, считано от получаване на писмената заявка по чл. 1, ал. 2 от проекта на договор за обществена поръчка.*

4.2. Срокът на гаранционно обслужване е 5 години, считано от датата на приемо-предавателния протокол за доставка.

***Забележка**: Участникът следва да предложи в офертата си срок за гаранционно обслужване, който следва да бъде минимум 5 (пет) години, считано от датата на подписване на двустранен приемо-предавателен протокол за приемане на доставката.*

5. Място на изпълнение

5.1. Потвърждаваме, че мястото на извършване на доставката е на територията на гр. София, като сме запознати, че ще бъде посочено в писмената заявка конкретния адрес на извършване на доставката.

5.2. Гаранционното обслужване ще се извършва спрямо местонахождението на доставеното и инсталиран софтуер.

6. Други изисквания

6.1. Декларираме, че сме надлежно упълномощени да извършваме доставка и гаранционно обслужване на предлагания от нас софтуер, необходим за обновяване на информационни и

комуникационни системи на територията на Република България.

За удостоверяване на горното представяме **Оторизационно писмо от производителя FORCEPOINT** (моля, посочете описание на документа)

Забележка: *За удостоверяване на горното участникът следва да представи Официално оторизационно писмо (или еквивалентен документ) с актуална дата от производителя или от официален представител на производителя на предлагания софтуер. Горепосоченият документ се представя в техническото предложение на участника.*

В случаите на представяне от участника на оторизационно писмо от официален представител на производителя (или еквивалентен документ), в офертата се прилага и оторизационно писмо, издадено от производителя (или еквивалентен документ), с което се упълномощава официалния представител на производителя за доставка и гаранционно обслужване на предлагания софтуер.

6.2. Прилагаме общи условия или други приложими условия за гаранционно обслужване от производителя на софтуера, предмет на обществената поръчка в случай, че е приложимо.

Дата на подписване:	**13/ 07/ 2020 г.**
Подпис и печат:	.....
Име и фамилия	**Николай Йорданов**
Длъжност	**Изпълнителен директор**
Наименование на участника	**Контракс АД**

КОНТРАКС АД 1

Интерлингва Варна ЕООД
Агенция за преводи

Варна, 9000
ул. Тракия -10, ап.7
Тел: (052) 631816
Тел/Факс: (052) 604972
e-mail: office@interlingua-bg.com
val@evko.com
Мобилен: 088 8534542

Превод от английски език

Forcepoint

Дата: 18.06.2020 г.
До:
„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД
Ул. „Панайот Волов“ 2
София 1504
България
Относно: „„„Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите“ Ref № 05948-2020-0004, ОП 7 „„„Доставка на система за защита от изтичане/загуба на данни от крайните точки и от мрежата“

ПИСМО ЗА УПЪЛНОМОЩАВАНЕ

Уважаеми Дами и Господа,

Със следното, ние, Forcepoint, с офис и адрес на регистрация в Пулавска 145, 02-715, Варшава, декларираме, че:
КОНТРАКС АД, с офис и адрес на регистрация: ул. „Тинтява“ 13, 1113 София, България, са упълномощени да участват в обществена поръчка с предмет: „Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите“ Ref № 05948-2020-0004, ОП 7 „„„Доставка на система за защита от изтичане/загуба на данни от крайните точки и от мрежата“ и да подпишат договор за доставка и пускане в действие на предлаганото оборудване с марка Forcepoint, за територията на Република България, съгласно политиката на Forcepoint, в пълно съответствие с одобрената тръжна документация на Възложителя. С настоящото ние разширяваме настоящото упълномощаване с това Оферента да изпълнява гаранционно обслужване на оборудването/ системите и да осигурява Ниво 1 на поддръжка. Оферентът ще осигури пълна гаранция и гаранционно обслужване съгласно нашия стандарт Споразумение за лиценз на краен потребител за продуктите, предлагани и доставени от тях.

Данните в настоящото писмо за поверителни за Forcepoint и се разкриват при условия на поверителност.

Дата: 18.06.2020 г.

Упълномощен подписващ:
(подпис – не се чете)

Долуподписаната [redacted] *удостоверявам верността на настоящия превод от английски на български език на приложения документ - [Forcepoint Authorisation – 1 стр].*
Преводът се състои от 1 (една) страница.
Заклет преводач: [redacted]

ВЯРНО С ОРИГИНАЛА
КОПИРАКС АД

Forcepoint

Date: 18.06.2020

To:
INFORMATION SERVICES JSC
2 Panayot Volov Str.
Sofia 1504
Bulgaria

Subject: "Delivery of communication equipment, hardware and software, required for the update of the information and communication systems of the National Revenue Agency" with Ref № 05948-2020-0004,

LOT 7 "Delivery of a protection system against endpoints and network data leakage / data los"

AUTHORIZATION LETTER

Dear Ladies and Gentleman,

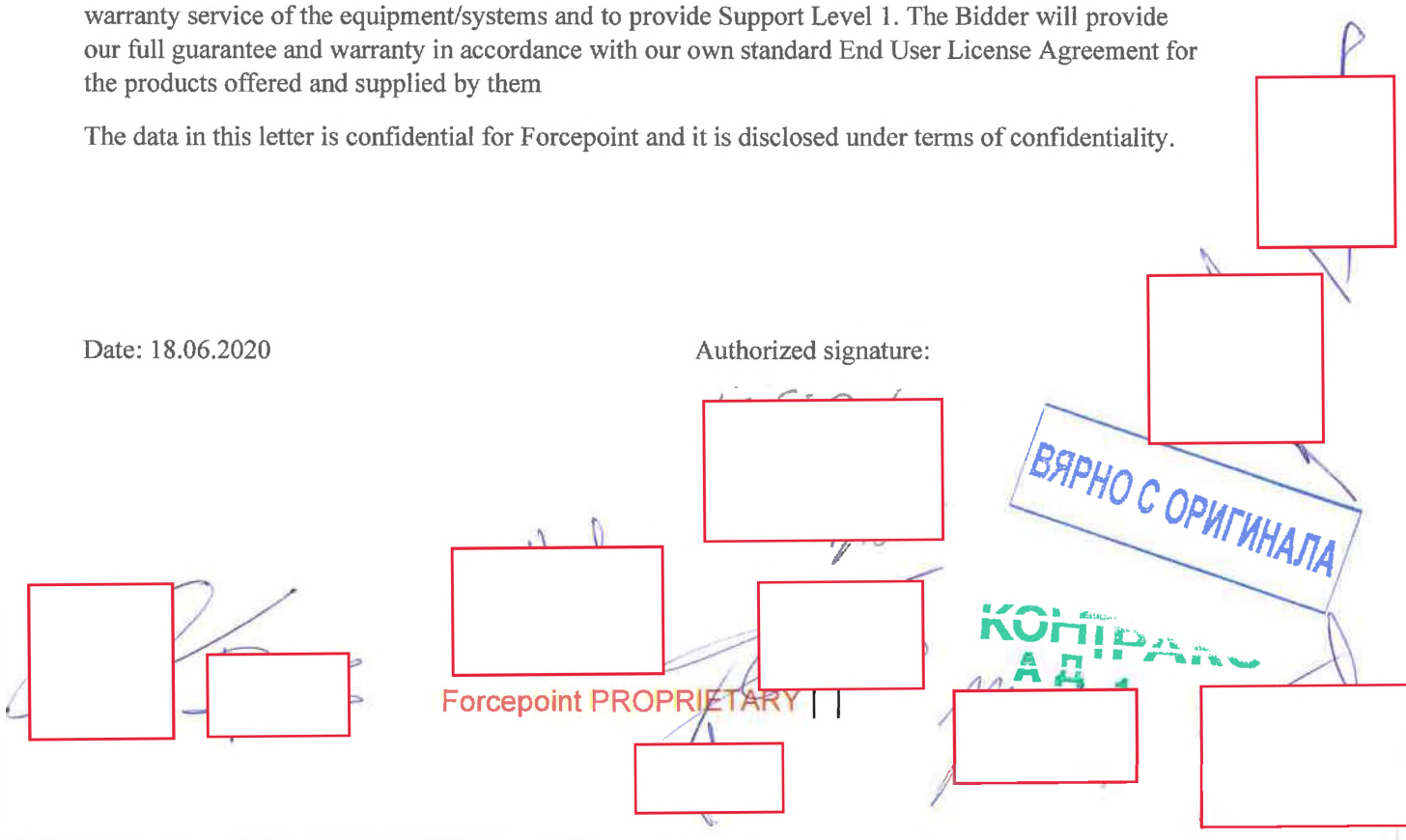
With the following, we Forcepoint, with registered office and address at Puławska 145, 02-715 Warszawa declare that:

KONTRAX AD, with registered office and address at 13 Tintyava Str., 1113 Sofia Bulgaria, is authorized to participate at public procurement procedure with subject "Delivery of communication equipment, hardware and software, required for the update of the information and communication systems of the National Revenue Agency" with Ref № 05948-2020-0004, LOT 7 "Delivery of a protection system against endpoints and network data leakage / data los" and to sign a contract for delivery and commissioning of equipment proposed by Forcepoint brand for the territory of the Republic of Bulgaria, according to the policy Forceopoint, in full accordance with the approved public documentation by the Assignor. We hereby extend the authorization for the Bidder to perform the warranty service of the equipment/systems and to provide Support Level 1. The Bidder will provide our full guarantee and warranty in accordance with our own standard End User License Agreement for the products offered and supplied by them

The data in this letter is confidential for Forcepoint and it is disclosed under terms of confidentiality.

Date: 18.06.2020

Authorized signature:



Forcepoint
Предотвратяване загубата на данни (DLP)

Защита на данните в свят без ограничения

FORCEPOINT

Forcepoint DLP

СИГУРНОСТ, ЗАДВИЖВАНА ОТ ЧОВЕКА

Сигурността на данните е непрекъснато предизвикателство. От една страна, от ИТ организациите се изисква да отговарят на изискванията на регулациите и да защитават интелектуалната собственост от целенасочени атаки и случайни излагания на риск. От друга страна, те трябва да се адаптират към макро движенията в ИТ сферата като например използването на облачни приложения, хибридни облачни среди и BYOD тенденции, като всички те увеличават начините, по които данните могат да напуснат Вашата организация.

Тези разширяващи се възможности за атака представляват най-голямото предизвикателство за защита на критични данни. Екипите по сигурността на данните използват привидно логичния подход за проследяване на данни: намират ги, включват ги в каталог и ги контролират. Въпреки това, този традиционен подход за предотвратяване на загубата на данни вече не е ефективен, защото игнорира най-голямата променлива в сигурността на данните – Вашите служители.

Вместо да се фокусира само върху данните, сигурността трябва да започва и завършва с хората. Ключът е да се осигури видимост върху работата на потребителя с данни и приложения. След като това бъде постигнато, можете да приложите ниво на контрол, определено на база специфичния риск на потребителя и чувствителността или стойността на данните.

Програмата за защита на данните на организацията трябва да разгледа човешката гледна точка - пресечната точка между потребители, данни и мрежи. В допълнение, организацията трябва да продължи да наблюдава данните, докато те се движат през нейната структура и да обърне специално внимание на хората, които създават, променят и преместват данни.

Защитата на данните трябва:

- **Да защити данни обект на регулации чрез централизирано управление за всички приложения, които Вашите служители използват, за да създават, съхраняват и преместват данни.**
- **Да защити интелектуалната собственост чрез напреднала DLP технология, която анализира как хората използват данни, обучава Вашите служители да взимат добри решения по отношение на данните и дава приоритет на инцидентите въз основа на риска.**

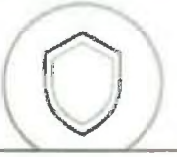
Видимост и контрол навсякъде, където работят Вашите служители и където се намират данните

- Облачни приложения (защита чрез Forcepoint CASB модул)
- Крайна точка
- Мрежа
- Откриване на данни „в покой" (Discovery)

Ускорява спазването на регулациите

Дава възможност на служителите да защитават данните

Усъвършенствано откриване и контрол на данните



Реагиране на инциденти и намаляване на риска

Forcepoint DLP адресира риска, породен от човешката намеса с видимост и контрол навсякъде, където работят Вашите служители и навсякъде, където се намират Вашите данни. Екипите по сигурността прилагат оценка на риска от потребителя, за да се фокусират върху събитията, които са най-важни и да ускорят спазването на глобалните регулации за данните.

Ускорено спазване на регулациите

Съвременната ИТ среда представлява ежедневно предизвикателство за предприятията, които се стремят да се съобразят с десетки глобални регулации за сигурност на данните, особено когато преминават към облачни приложения и мобилна работна сила. Много решения за сигурност предлагат някаква форма на интегрирано DLP, като например DLP технологията в облачните приложения. Въпреки това, екипите по сигурността са изправени пред нежеланото усложнение и допълнителни разходи при налагане и управление на отделни и непоследователни политики в крайните точки, облачните приложения и мрежите.

Forcepoint DLP ускорява Вашите усилия за спазване на регулациите, като комбинира предварително зададени правила за покриване на глобални регламенти с централизиран контрол на Вашата ИТ среда.

Forcepoint DLP ефективно защитава чувствителната Ви информация и регулираните Ви данни, така че да можете уверено да докажете текущо съответствие с изискванията.

- Покритие на регулаторните изисквания чрез използване на над 350 предварително зададени политики, приложими за доказване на съответствие с регулациите на повече от 80 държави
- Намиране и отстраняване на проблеми с регулирани данни чрез сканиране на мрежата, облачните среди и крайните точки
- Централизиран контрол и единни политики за цялата ИТ среда

Дава възможност на служителите да защитават данните

DLP решенията, които използват само превантивни правила, създават неудобства за потребителите, които ще ги заобиколят с единственото намерение да изпълняват задачите си. Заобикалянето на сигурността води до нежелано излагане на риск на данните.

Forcepoint DLP разпознава Вашите служители като първа линия в борбата с днешните кибер заплахи.

- Открива и контролира данните навсякъде, където те се намират, независимо дали са в облачни среди или в локалната мрежа, в имейл или на крайните точки.
- Обучава служителите да взимат интелигентни решения, чрез използване на съобщения, които ръководят действията на потребителите, обучават служителите относно политиките и валидират намеренията на потребителите при взаимодействие с критични данни.
- Предоставя сигурност при сътрудничеството с доверени партньори, използвайки базирано на политики автоматично криптиране на данните, които се движат в посока извън мрежата на вашата организация.
- Автоматизира поставянето на етикети и класифицирането на данните чрез интегриране с водещи решения за класификация на данни на трети страни.

Protection, Boldon James, Titus).

Разширено откриване и контрол на данните, където и да се намират

Умишлените и случайните нарушения на политиките за сигурност на данните са сложни инциденти, а не единични събития. Forcepoint DLP е доказано решение, което аналитичните фирми, включително Gartner, Radicati и други, признават за лидер в индустрията. DLP решенията на Forcepoint се предлагат в 2 варианта: DLP за съответствие (Compliance) и DLP за защита на интелектуалната собственост (IP).

Forcepoint DLP за съответствие осигурява функционалности от критична важност като например:

- Оптичното разпознаване на символи (OCR) идентифицира данни, вградени в изображения, докато са в покой или в движение.
- Надеждната идентификация на лична информация (PII) предлага проверки за валидиране на данни, откриване на реално време, анализ на базата на частично сходство на данните и откриване на контекста.
- Възможност за откриване на криптирани данни, които опитват да избегнат откриване при сканиране и да избегнат наложените политики за сигурност.
- Кумулативен анализ за откриване на частично изтичане на данни (Drip DLP - т.е. данни, които изтичат на части, за дълъг период от време).
- Интеграцията с Microsoft Azure Information Protection анализира криптирани файлове и прилага подходящи DLP контроли към данните.

Forcepoint DLP за защита на интелектуалната собственост включва възможностите по-горе, като същевременно предоставя сложни алгоритми за откриване и контрол на потенциална загуба на данни с функции като например:

- Машинно обучение, което позволява на потребителите да обучат системата да идентифицира подходящи, никога не виждани досега данни. Потребителите предоставят положителни и отрицателни примери за маркиране на сходни бизнес документи, програмен код и други.
- Поставяне на „пръстов отпечатък" на структурирани и неструктурирани данни позволява на собствениците на данните да определят типа на данните и да идентифицират пълни и частични съвпадения в бизнес документи и в бази от данни, като след това да прилагат правилните контроли или политики, които съответстват на данните.
- Анализ за откриване на промените в поведението на потребителя, когато то е свързано с взаимодействие с данни, като например по-често използване на личен имейл адрес за изпращане на съобщения.

Намаляване и отстраняване на риска

Традиционните DLP технологии претоварват потребителите с грешни показания, като същевременно пропускат реалните рискове, свързани с работата с данни. Forcepoint DLP предоставя разширен анализ, за да съпостави на пръв поглед несвързани DLP събития в приоритетни инциденти. Поставянето на оценка на риска от инциденти (IRR), част от Forcepoint DLP, съчетава различни DLP индикатори в Байесовски мрежи, за да се оцени степента на риск за данните при различни сценарии, като например кражба на данни и нарушаване на бизнес процеси.

- Фокусира екипите за реакция върху най-големите рискове чрез маркиране на приоритетни инциденти, като се акцентира върху рисковите потребители, изложените на риск критични данни и сходните модели на поведение измежду потребителите.
- Разследване и реагиране чрез спързване на различни събития, показване на контекста на рисковите данни и предоставяне на информация на анализаторите, която им е необходима за предприемане на действия.
- Защита на поверителността на потребителите чрез възможност за анонимизация на данните и контрол на достъпа.
- Добавя контекста на данните за извършване на по-широк анализ на потребителите чрез директна интеграция с Forcepoint Insider Threat и Forcepoint Behavioral Analytics.

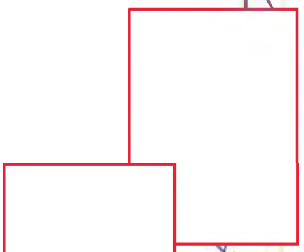
Видимост навсякъде, където работят Вашите служители, контролирайте навсякъде, където са Вашите данни

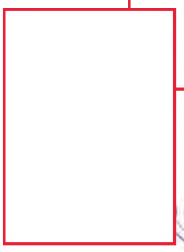
Днес предприятията са изправени пред трудностите, свързани с използването на сложни среди, където данните са разположени навсякъде и се изисква защита на данните на места, които не се управляват или притежават от предприятието. Forcepoint DLP за облачни приложения предоставя по-широк анализ и DLP политики за критични облачни приложения, така че Вашите данни да бъдат защитени, където и да се намират.

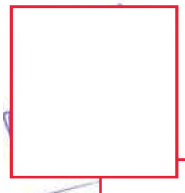
- Идентифициране и защита на данни в облачни приложения, мрежови хранилища на данни, бази от данни и управлявани крайни точки.
- Видимост над качванията и свалянията на данни, както и споделянето и съхраняването на данни в най-популярните облачни приложения, използвани от предприятията, включително Office 365, Google Apps, Box, Salesforce и други.
- Обединява прилагането на политики чрез единична конзола, за да определите и приложите политики във всички канали - CLOUD, мрежа и крайни точки.
- Forcepoint решения, които предоставят DLP функции за поставяне на „пръстови отпечатъци" и алгоритми за машинно обучение за облачни приложения.

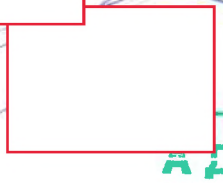
Forcepoint DLP включва разширен анализ и налагане на регулаторни политики чрез използване на

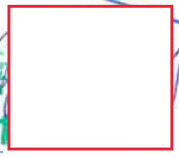
избират измежду вариантите за внедряване на решението според тяхната ИТ среда

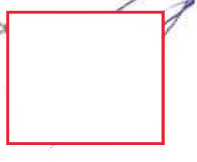


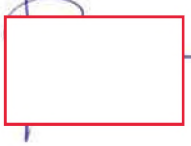












ВЯРНО С ОРИГИНАЛА

Приложение А: Forcepoint DLP – РАЗГЛЕЖДАНЕ НА КОМПОНЕНТИТЕ НА РЕШЕНИЕТО

Forcepoint DLP за крайни точки	Forcepoint DLP защитава вашите критични данни в крайните точки на Windows и Mac в и извън корпоративната мрежа. Включва усъвършенствана защита и контрол на данни в покой (откриване), в движение и в употреба. Той се интегрира с Microsoft Azure Information Protection за анализ на криптирани данни и прилагане на подходящи DLP контроли. Дава възможност на служителя за самокорекция на риска върху данните въз основа на ръководство от диалоговия прозорец за DLP. Решението следи уеб качванията на данни, включително HTTPS, както и качванията на данни в облачни услуги като Office 365 и Box Enterprise. Пълна интеграция с Outlook, Notes и имейл клиенти.
Forcepoint DLP за облачни приложения	Forcepoint CASB, DLP за облачни приложения, разширява усъвършенстваният анализ и единния контрол върху Forcepoint DLP към критични облачни приложения, включително Office 365, Salesforce, Google Apps, Box, ServiceNow и други.
Forcepoint DLP Discovery	Forcepoint DLP открива, идентифицира и подсигурява чувствителни данни във вашата мрежа, както и данни, съхранявани в облачни услуги като Office 365 и Box Enterprise. Разширената технология за поставяне на „пръстови отпечатъци" идентифицира регулирани данни и интелектуална собственост „в покой" и защитава тези данни чрез прилагане на подходящо криптиране и контрол.
Forcepoint DLP за мрежова защита	Forcepoint DLP Network предоставя мрежова защита, за да спре кражбата на данни „в движение" чрез имейл и интернет канали. Решението помага да се идентифицират и предотвратят умишлени и случайни загуби на данни от външни атаки или от нарастващите вътрешни заплахи. OCR (оптично разпознаване на символи) разпознава данни в рамките на изображение. Анализът идентифицира опитите за изнасяне на информация, за да спре кражбата на данни чрез частично изнасяне през голям период от време, както и чрез други рискови действия на потребителите.

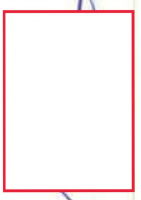
Приложение Б: Forcepoint DLP – подробни детайли за компонентите

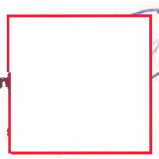
	Forcepoint DLP – Endpoint	Forcepoint DLP – Cloud Applications	Forcepoint DLP – Discovery	Forcepoint DLP – Network
Как се внедрява?	Forcepoint One агент	Разположено в Forcepoint Cloud	IT Managed Discovery Server	Мрежово устройство или Public Cloud

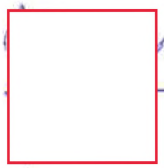
Как се управлява?	Чрез Forcepoint SECURITY Manager (FSM) за конфигуриране и налагане на политики от единна конзола за управление. Може да се инсталира локално или в рамките на PUBLIC CLOUD (AWS или Azure)			
Каква е основната функция?	Предотвратяване загубата на данни за крайните точки, откриването на данни и автоматизираната класификация на данните.	Видимост на движението на данни и прилагане на политиките в управлявани облачни приложения	Откриване и сканиране на данни „в покой", в центрове за данни и в облачни приложения	Видимост и контрол на данните „в движение", изпратени чрез уеб и имейл трафик
Къде са открити данните / защитени данните „в покой"?	Windows крайни точки MacOS крайни точки Linux крайни точки	Exchange Online Sharepoint Online Box	Локални файлови сървъри и мрежови масиви Sharepoint Server Online Exchange Server Online Box Enterprise	
Къде са защитени данните „в движение"?	Имейл, уеб: HTTP (S), принтери, преносими носители, Мобилни устройства, Файлови сървъри / NAS	Качвания, сваляния и споделяне в Office 365, Google Apps, Salesforce.com, Box & ServiceNow		Web: HTTP(S) ICAP
Къде са защитени данните „в употреба"?	IM, VOIP, приложения (клиенти за облачно съхранение), клипборд на ОС	В ТЕЧЕНИЕ НА ДЕЙНОСТИТЕ ЗА СЪТРУДНИЧЕСТВО, ИЗПОЛЗВАЩИ ОБЛАЧНИ ПРИЛОЖЕНИЯ		
Определяне на риска на инцидентите	Включено	Включено		Включено
Оптично разпознаване на символи			Включено	Включено

ВЯРНО С ОРИГИНАЛА

Класифициращи ни данни и интеграция с решения за поставяне на етикети	Microsoft Azure Information Protection, Boldon James, Titus
На какви данни може да бъде сложен „пръстов отпечатък"?*	Структурирани (бази от данни), неструктурирани (файлови документи), двоичен код (нетекстови файлове)
Глобална библиотека от политики за сигурност	Откриване на данни и налагане на правила за сигурност от глобална библиотека с множество политики, спомагащи за съответствие с наложените регулации







ВЯРНО С ОРИГИНАЛА

КОНТРАКС АД

За Forcepoint

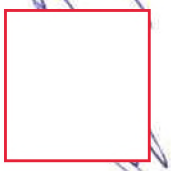
Forcepoint е глобална компания за киберсигурност фокусирана върху хората, преобразуваща дигиталната информаци на предприятията чрез непрекъснато адаптиране на сигурността към динамичния риск, породен от индивидуал потребители и машини. Решенията на Forcepoint, фокусирани върху поведението на потребителите, осигуряв сигурност, адаптирана към риска, за непрекъсната защита на данни и системи. Базирана в Остин, Тексас, Forcepoint защитава данните на хиляди предприятия и правителства в над 150 страни.

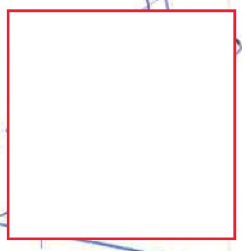
forcepoint.com/contact

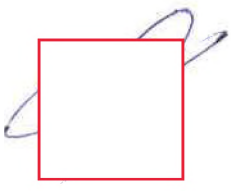
[DATA LOSS PREVENTION-GLOBAL-BROCHURE-US-EN] 400004.110419

FORCEPOINT

Подписаната, Антония Миланова Василева, ЕГН: 8105278498, Потвърждение № 18ПР-1398/26.02.2018 г., удостоверявам верността на превода от английски на български език на приложения документ, извършен от мен. Преводът се състои от 8страници.
Подпис: Антония Миланова Василева







Forcepoint Data Loss Prevention (DLP)

Data protection in a zero-perimeter world

FORCEPOINT

Forcepoint DLP

SECURITY driven by the HUMAN point

Data SECURITY is a never-ending challenge. On one hand, IT organizations are REQUIRED to keep UP with REGULATIONS and protect INTELLECTUAL property from targeted attacks and accidental EXPOSURE. On the other, they MUST adapt to macro IT movements, SUCH as the adoption of CLOUD applications, hybrid CLOUD environments and BYOD trends, all of which increase the ways data can leave YOUR organization.

This expanding attack SURFACE poses the most significant challenge to protecting critical data. Data SECURITY teams take the seemingly logical approach to chase data: find it, CATALOGUE it and control it. Yet this traditional approach to data loss prevention is no longer effective BECAUSE it ignores the biggest variable in data SECURITY — YOUR people.

Instead of FOCUSING solely on data, SECURITY SHOULD begin and end with people. The key is to gain visibility into USER interactions with data and applications. Once this is achieved, YOU CAN apply a level of control based on the specific USER's risk and the sensitivity or VALUE of the data.

An organization's data protection program MUST consider the HUMAN point — the intersection of USERS, data and networks. In addition, the enterprise MUST remain vigilant of data as it moves across the enterprise and highlight the people who create, TOUCH and move data.

Data protection MUST:

- **SECURE REGULATED data** with a single point of control for all the applications YOUR people USE to create, store and move data.
- **Protect INTELLECTUAL property** with advanced DLP that analyzes how people USE data, **coaches** YOUR people to make good decisions with data and prioritizes incidents by risk.

Visibility & control everywhere YOUR people work and data resides

- CLOUD Applications (powered by Forcepoint CASB)
- Endpoint
- Network
- Discovery

Accelerate Compliance

Empower People to Protect Data

Advanced Detection & Control

Respond & Remediate Risk

Forcepoint DLP addresses HUMAN-CENTRIC risk with visibility and control everywhere YOUR people work and everywhere YOUR data resides. SECURITY teams apply USER-risk scoring to FOCUS on the events that matter most and to accelerate compliance with global data REGULATIONS.

Accelerate compliance

The modern IT environment presents a DAUNTING challenge for enterprises aiming to comply with dozens of global data SECURITY REGULATIONS, especially as they move toward CLOUD applications and mobile workforces. Many SECURITY SOLUTIONS offer some form of integrated DLP, SUCH as the type FOUND within CLOUD applications. Yet SECURITY teams face UNWANTED complexity and added costs when deploying and managing separate and inconsistent policies across endpoints, CLOUD applications and networks.

Forcepoint DLP accelerates YOUR compliance efforts by combining pre-packaged coverage of global REGULATIONS with central control across YOUR IT environment. Forcepoint DLP efficiently SECURES sensitive CUSTOMER information and REGULATED data so YOU CAN confidently prove ongoing compliance.

- REGULATORY coverage to QUICKLY meet and maintain compliance with over 350 policies applicable to the REGULATORY demands of more than 80 COUNTRIES.
- Locate and remediate REGULATED data with network, CLOUD and endpoint discovery.
- Central control and consistent policies across the IT environment.

Empower people to protect data

DLP with only preventive controls FRUSTRATES USERS who will CIRCUMVENT them with the sole intention of completing a task. Going AROUND SECURITY RESULTS in UNNECESSARY risk and inadvertent data EXPOSURE.

Forcepoint DLP recognizes YOUR people as the front lines of today's cyber threats.

- Discover and control data everywhere it lives, whether in the CLOUD or on the network, via email and at the endpoint.
- Coach employees to make smart decisions, USING messages that GUIDE USER actions, EDUCATE employees on policy and validate USER intent when interacting with critical data.
- SECURELY collaborate with TRUSTED partners USING policy-based AUTO-encryption that protects data as it moves OUTSIDE YOUR organization.
- AUTOMATE data labeling & classification by integrating with leading third-party data classification SOLUTIONS (e.g., Microsoft AZURE Information Protection, Boldon James, TITUS).

Advanced detection and controls that follow the data

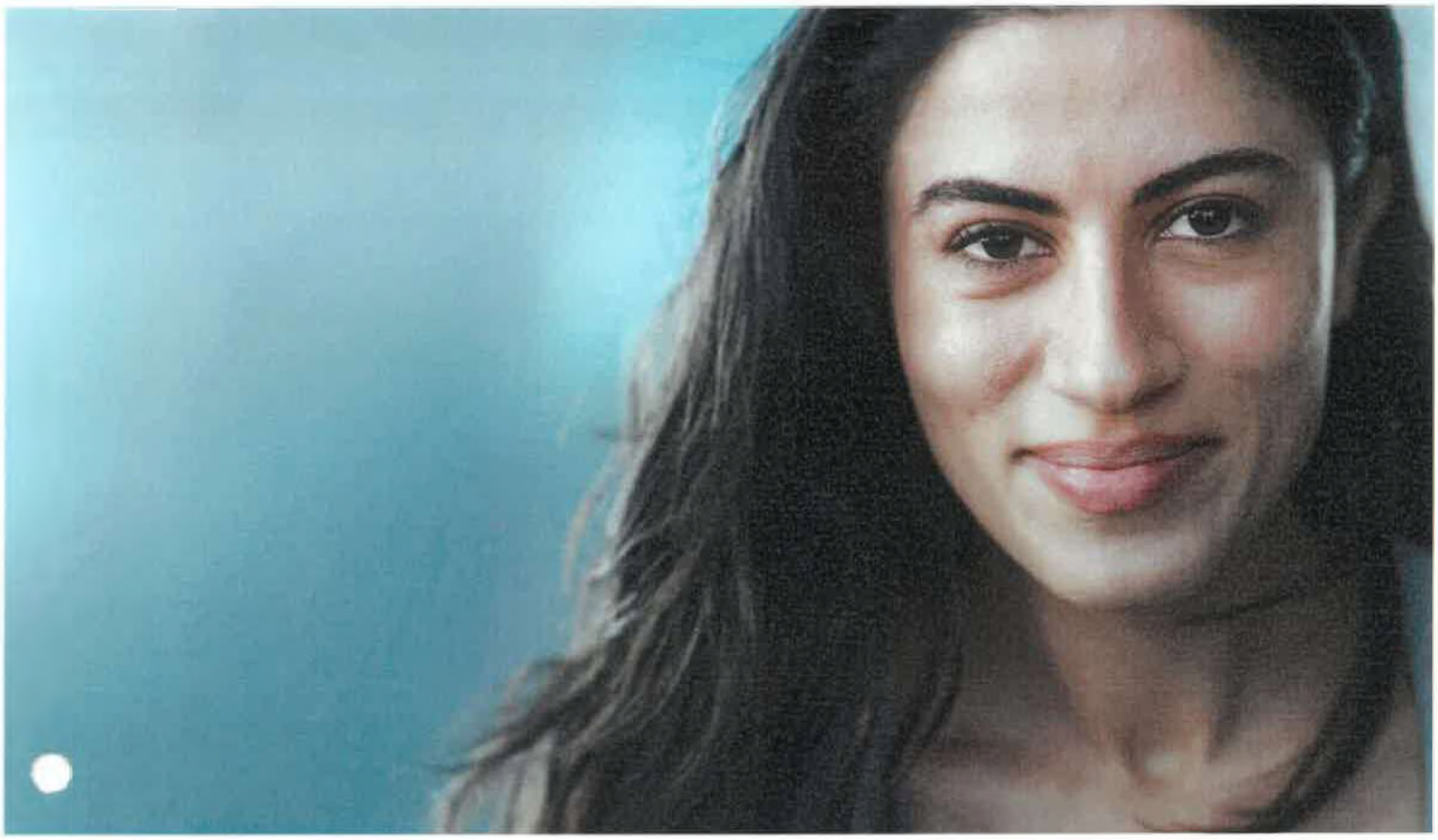
MALICIOUS and accidental data breaches are complex incidents, not single events. Forcepoint DLP is a proven SOLUTION that analyst firms INCLUDING Gartner, Radicati and others recognize as a leader within the INDUSTRY. Forcepoint's DLP offerings are available in 2 versions: DLP for Compliance and DLP for INTELLECTUAL Property (IP) Protection.

Forcepoint DLP for Compliance provides critical capability addressing compliance with FEATURES SUCH as:

- Optical Character Recognition (OCR) identifies data imbedded in images while at rest or in motion.
- ROBUST identification for Personally Identifiable Information (PII) offers data validation checks, real name detection, proximity analysis and context identifiers.
- CUSTOM encryption identification exposes data hidden from discovery and applicable controls.
- CUMULATIVE analysis for drip DLP detection (i.e., data that leaks OUT slowly over time).
- Integration with Microsoft AZURE Information Protection analyzes encrypted files and applies appropriate DLP controls to the data.

Forcepoint DLP for IP Protection INCLUDES the capabilities above, PLUS applies the most advanced detection and control of potential data loss with FEATURES SUCH as:

- Machine learning allows USERS to train the system to identify relevant, never-before-seen data. Users provide the engine with positive and negative examples to flag similar BUSINESS DOCUMENTS, SOURCE code and more.
- Fingerprinting of STRUCTURED and UNSTRUCTURED data allows data owners to define data types and identify FULL and partial matches across BUSINESS/DOC design plans and databases, and then apply control or policy that matches the data.
- Analytics identify changes in USER behavior as it relates to data interaction SUCH as increased USE of personal email.



Respond and remediate risk

Traditional approaches to DLP overload USERS with false positives while missing data at risk. Forcepoint DLP applies advanced analytics to correlate seemingly UNRelated DLP events into prioritized incidents. Incident Risk Ranking (IRR) provided with Forcepoint DLP FUSES disparate DLP indicators into a framework of Bayesian belief networks to assess the likelihood of data risk scenarios, SUCH as data theft and broken BUSINESS processes.

- **Focus response teams on greatest risk** with prioritized incidents that highlight the people responsible for risk, the critical data at risk and common patterns of behavior across USERS.
- **Investigate and respond** with workflows that link disparate events, show context of data at risk and provide analysts with the information they need to take action.
- **SafeGUARD USER privacy** with anonymization options and access controls.
- **Add the context of data** into broader USER analytics THROUGH deep integrations with Forcepoint Insider Threat and Forcepoint Behavioral Analytics.

Visibility everywhere YOUR people work, control everywhere YOUR data resides

Today's enterprises are challenged with complicated environments, where data is everywhere and REQUIRES the protection of data in places that aren't managed or owned by the enterprise. Forcepoint DLP for CLOUD Applications extends analytics and DLP policies to critical CLOUD applications so YOUR data is protected, wherever it resides.

- **Identify and protect data** across CLOUD applications, network data stores, databases and managed endpoints.
- **Gain visibility** to UPLOADS and downloads as well as data sharing and stored data on the most POPULAR CLOUD apps UTILIZED by enterprises INCLUDING Office 365, Google Apps, Box, Salesforce and more.
- **Unify policy enforcement** via single console to define and apply policies across all channels - CLOUD, network and endpoints.
- **Forcepoint hosted** SOLUTION that extends enterprise DLP FEATURES INCLUDING fingerprinting and machine learning to CLOUD applications.

Forcepoint DLP INCLUDES advanced analytics and REGULATORY policy templates from a single point of control with deployment. Enterprises choose the deployment o for their IT environment.

Appendix A: DLP SOLUTION component overview

Forcepoint DLP – Endpoint	Forcepoint DLP – Endpoint protects YOUR critical data on Windows and Mac endpoints on and off the corporate network. It INCLUDES advanced protection and control for data at rest (discovery), in motion and in USE. It integrates with Microsoft AZURE Information Protection to analyze encrypted data and apply appropriate DLP controls. Enables employee self-remediation of data risk based on GUIDANCE from DLP coaching dialog. The SOLUTION monitors web UPLOADS, INCLUDING HTTPS, as well as UPLOADS to CLOUD services like Office 365 and Box Enterprise. FULL integration with OUTLOOK, Notes and email clients.
Forcepoint DLP – CLOUD Applications	Powered by Forcepoint CASB, DLP – CLOUD Applications extends the advanced analytics and single control of Forcepoint DLP to critical CLOUD applications, INCLUDING Office 365, Salesforce, Google Apps, Box, ServiceNow and more.
Forcepoint DLP – Discovery	Forcepoint DLP – Discovery identifies and SECURES sensitive data across YOUR network, as well as data stored in CLOUD services like Office 365 and Box Enterprise. Advanced fingerprinting technology identifies REGULATED data and INTELLECTUAL property at rest and protects that data by applying appropriate encryption and controls.
Forcepoint DLP – Network	Forcepoint DLP – Network delivers the critical enforcement point to stop the theft of data in motion THROUGH email and web channels. The SOLUTION helps identify and prevent MALICIOUS and accidental data loss from OUTSIDE attacks or from the growing insider threats. OCR (Optical Character Recognition) recognizes data within an image. Analytics identify DLP to stop the theft of data one record at a time and other high-risk USER behaviors.

Appendix B: DLP SOLUTION components detail

	Forcepoint DLP – Endpoint	Forcepoint DLP – CLOUD Applications	Forcepoint DLP – Discover	Forcepoint DLP – Network
How is it deployed?	Forcepoint One Endpoint	Hosted in Forcepoint CLOUD	IT Managed Discovery Server	Network Appliance or PUBLIC CLOUD
How is it managed?	Via Forcepoint SECURITY Manager (FSM) for single console policy CONFIGURATION & enforcement. This can be deployed on-premises or within PUBLIC CLOUD (AWS or AZURE)			
What is the primary FUNCTION?	Prevention of endpoint data loss, data discovery and AUTOMATED data classification.	Visibility of data movement and enforcement of policies in sanctioned CLOUD applications	Discovery, scanning and remediation of data at rest within data centers and CLOUD applications	Visibility and control for data in motion via the web and email
Where is the data discovered / protected at rest?	Windows endpoints MacOS endpoints LINUX endpoints	Exchange Online Sharepoint Online Box	On-premises file servers and network storage Sharepoint Server Online Exchange Server Online Box Enterprise	
Where is data in motion protected?	Email, Web: HTTP(S), Printers, Removable media, Mobile devices, File servers / NAS	Uploads, downloads & sharing on Office 365, Google Apps, Salesforce.com, Box & ServiceNow		Web: HTTP(S) ICAP
Where is data in USE protected?	IM, VOIP file sharing, applications (CLOUD storage clients), OS clipboard	DURING collaboration activities USING CLOUD applications		
Incident risk ranking	INCLUDED	INCLUDED		INCLUDED
Optical character recognition			INCLUDED	INCLUDED
Data classification & labeling integrations	Microsoft AZURE Information Protection, Boldon James, TITUS			
What data can be fingerprinted?*	STRUCTURED (databases), UNSTRUCTURED (DOCUMENTS), Binary (non-TEXTUAL files)			
Global policy library	Discovery & enforcement from broad compliance policy library			

About Forcepoint

Forcepoint is the global HUMAN-CENTRIC CYBERSECURITY company transforming the digital enterprise by CONTINUOUSLY adaptin SECURITY response to the dynamic risk posed by INDIVIDUAL USERS and machines. The Forcepoint HUMAN point system delivers risk-adaptive protection to CONTINUOUSLY ENSURE TRUSTED USE of data and systems. Based in AUSTIN, Texas, Forcepoint protects the HUMAN point for THOUSANDS of enterprise and government CUSTOMERS in more than 150 COUNTRIES.

forcepoint.com/contact

[DATA LOSS PREVENTION-GLOBAL-BROCHURE-US-EN] 400004.110419

FORCEPOINT

ОБЩИ УСЛОВИЯ

за гаранционно обслужване от производителя **FORCEPOINT**
на продуктите, предмет на обществената поръчка **„Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите'',**
по Обособена позиция № 7: „Доставка на система за защита от изтичане/загуба на данни от крайните точки и от мрежата“

Настоящите гаранционни условия се отнасят за дефекти, възникнали в следствие процеса на нормална експлоатация по време на гаранционния период. Гаранционният срок на софтуерните продукти започва да тече от датата на издаване на лицензионния сертификат от производителя и обхваща периода зададен в сертификата.

Производителят **FORCEPOINT** доставя своите софтуерни продукти с Подсилено ниво на поддръжка (**Forcepoint Enhanced Support**). Подсиленото ниво на поддръжка осигурява софтуерна поддръжка от типа 24x7x365. Времето за реакция на производителя при критични проблеми е до два бизнес дена.

Подсилената поддръжка включва:

- 24x7 достъп до защитен онлайн портал за поддръжка (Secure Support Portal), който предоставя:
  - Възможност за конфиденциално изпращане на заявки за извършване на техническа поддръжка, свързани със закупените софтуерни решения, за преглед от техническия екип на производителя;
  - Обратна връзка от техническия екип по докладваните технически неизправности и въпроси. Възможност за комуникация по няколко канала: електронна поща, телефонно обаждане;
  - Възможност за разглеждане на комуникацията относно активните заявки за техническа поддръжка и придобитата информация;
  - Достъп до форум общност от клиентите на производителя за обсъждане на теми свързани с техническа поддръжка;
- Достъп до обновления на софтуерните продукти на производителя за периода на поддръжката:

- Достъп до основни обновления на софтуерните продукти на производителя, включващи нови версии;
- Достъп до минорни обновления на софтуерните продукти на производителя, с малки корекции или подобрения;

- 24x7 достъп до онлайн портал с техническа документация на производителя, който предоставя:
  - Достъп до ръководства за инсталация и експлоатация на софтуерните решения;
  - Достъп до ръководства за преминаване към по-нова версия на софтуерните решения;
  - Достъп до документация с известия за функционалните изменения в най-новите версии на софтуерните решения;
- 24x7 глобална поддръжка за изпратени заявки за техническа поддръжка от степен 1 и от степен 2, които са с най-сериозен характер относно ограничена функционалност или спиране на работни процеси;
- Приоритет при отговарянето от производителя на заявки за техническа поддръжка за клиенти с Подсилена (Enhanced) поддръжка пред клиенти с Основна (Essential) поддръжка;
- Заделяне на обособено лице от производителя за по-бърза комуникация и ескалиране на заявки за техническа поддръжка за клиенти с Подсилена поддръжка;
- Възможност за годишен преглед от продуктови експерти на производителя, които проверяват състоянието на имплементираните софтуерни решения на производителя, като същевременно спомагат за отстраняването на технически неизправности и предоставят детайлен отчет с препоръки за оптимизиране на производителността на решенията;

Времената за реакция на техническия екип на производителя при подаване на информация з технически неизправности, при Подсилена поддръжка с достъпност тип 24x7x365, са както следва:

- За инциденти от степен 4 – минорни инциденти, които не водят до прекъсване на процеси и услуги на софтуерните продукти – отговор до 2 бизнес дена;

- За инциденти от степен 3 – средни или минорни инциденти, които водят до кратко прекъсване или неизправност на процеси и услуги на софтуерните продукти – отговор до 6 часа;
- За инциденти от степен 2 – големи инциденти, които водят до сериозно ограничаване или прекъсване на процеси и услуги на софтуерните продукти, но не спиращи изцяло работния процес на организацията – отговор до 2 часа;
- За инциденти от степен 1 – критични инциденти, които водят до трайно прекъсване на процеси и услуги на софтуерните продукти и спиране на работния процес на организацията – отговор до 45 минути;

Повече информация има на следния адрес:
https://www.forcepoint.com/sites/default/files/resources/files/datasheet_support_programs_2018_en_0.pdf

Контракс АД
София 1113, ул. Тинтява 13
тел.: (02) 960 9777; факс: (02) 960 9797
e-mail: sales@kontrax.bg; www.kontrax.bg

ОПИСАНИЕ НА СИСТЕМА ЗА ПРИЕМАНЕ И ОБСЛУЖВАНЕ НА СЕРВИЗНИ ЗАЯВКИ

Сервизната процедура на **Контракс АД** се базира на стандартите за управление ISO 9001:2015 и 20000-1:2011.

За осигуряване на услуги по гаранционна и извънгаранционна поддръжка Контракс разполага със Сервизен център (т.нар. Help Desk), който има задълженията да приема заявки от клиентите/потребителите и да управлява и контролира дейността на сервиза на Контракс по отстраняването на инцидентите и проблемите и обслужване на заявките на крайните потребители.

Ролята на звеното Сервизен център в Контракс, е да бъде единна точка на контакт за крайните потребители на компанията по отношение на инциденти и заявки, свързани с предоставяните от Контракс услуги.

Основните отговорности на Сервизния център включват:

- Обслужване на потребителите и клиентите;
- Регистриране и мониториране на инцидентите;
- Мониторинг и ескалация базирана на договорените Нива на сервизно обслужване;
- Първоначална оценка на инцидентите с цел тяхното решаване или пренасочване;
- Затваряне на инцидентите след потвърждение от потребителите;
- Управлява жизнения цикъл на сервизните заявки;
- Отчитане на нивата на предоставяне на услуги съгласно изискванията на Възложителя.

Всички събития, свързани с управление на инцидентите ще следват еднаква процедура: например наблюдение чрез наличната система за мониторинг, създаване на Билети за проблем в системата на Сервизния център. Центърът за услуги ще извършва класификация на инцидентите и разрешаването им в съответствие с договорените срокове. В случай, че е необходимо, ще се извърши ескалиране към определеното следващо ниво. Актуализациите на статуса на инцидента могат да бъдат предадени на Сервизния център по електронна поща или он-лайн, така че да се поддържа статуса на билета за проблем и отговорният служител на Възложителя да бъде уведомен по съгласуваните канали за комуникация, в това число чрез уеб-портал, е-мейл или телефон за наличието на инциденти и техният статус и развитие.

Инцидентите, докладвани на Сервизния център ще бъдат регистрирани директно в системата за управление на инциденти. Процедурите по управление на инцидентите преминават през актуализиране до приключване.

Извършваните дейности включват:

- Поемане на отговорността от начало до край, както и „собствеността" в[illegible] всеки инцидент, включително минимизиране на трансферите към повече екипи за поддръжка.
- Управляване и координиране на техническите средства и/или трети страни доставчици или изпълнителите за съдействие при отстраняването на инциденти,

възникнали от неочаквани прекъсвания на услугата.
- Възстановяване на услугите в рамките на изискваните от Възложителя.
- Информация за същността на инцидента и положените усилия от страна на поддържащия персонал за отстраняване му.
- Информиране на персонала на Възложителя за прекъсването на работата на използваните системи.
- Подаване на информация за статуса на инцидента към отговорния персонал в Възложителя при неговото отстраняване.
- Да осигури обратна информация към Възложителя под формата на доклади и анализи за управление на инцидентите.

Когато потребителската заявка не може да бъде разрешена от оператора, която я приема, се регистрира инцидент. Операторът ескалира проблема към съответната работна група с по-висока компетентност.

Инциденти се регистрират автоматично от системите за наблюдение на ИТ инфраструктурата ако такива има инсталирани. Автоматично се определя приоритета на инцидента и времето за неговото разрешаване. При регистрация на инцидент операторът внимателно определя компетентна работна група, отговорна за разрешаването на инцидента. Операторът може да посочи конкретно лице от работната група.

За да бъде насочен инцидента е необходимо да бъде посочена Работната група от системни инженери, към която се насочва проблема за разрешаване. Лице от работната група, поел проблема, става собственик на инцидента и е отговорно за неговото разрешаване от момента на получаването му.

Когато не е насочена към правилната работна група, лицето поело инцидента връща заявката към оператора на сервизния център. При такъв вид действие, специалистът на второ ниво е длъжен да опише защо счита, че случаят не е от компетентността на неговата група. Операторът насочва инцидента към друга работна група за разрешаване.

При приемане на инцидента Операторът на системата извършва следните действия:

1) Приема заявката от крайните потребители по телефон, E-mail или WEB регистрирана заявка.
2) Регистрира заявката в сервизната система. Попълва данните на крайния потребител и на засегнатата система.
3) Определя нивото на критичност на инцидента и го регистрира
4) Определя от чия компетентност е заявката за обслужване.

Времето за реакция е до следващия работен ден от уведомяването от клиента. „Време за реакция“ е времето от момента на уведомяване от страна на клиента за възникнал проблем до обратна реакция (обаждане или пристигане на място) от наша страна. Осигуряваме и преглед на място в срок не по-късно от следващия работен ден от 9.00 ч. до 17.30 ч.

Намеса от ниво 1

Процесът на диагностиране на инцидента започва с анализ на детайлите на инцидента, с цел идентифициране на подходяща поредица от действия за разрешаване на инцидент, възможно най-бързо. Сервизният инженер преглежда за други отворени инциденти, свързани с ИТ актива.

За бързо разрешаване на инцидента Сервизният инженер използва информация в Базата знания, която съдържа описание на решения за инциденти със сходно описание.

Сервизният инженер, отговорен за разрешаване на инцидента, отразява всички действия, извършени при отстраняването на проблема. Отразяват се предприети действия – комуникация с потребителя, анализ, изследване, комуникация с доставчик и др. подобни. По преценка на специалиста част от тази информация може да бъде видима за потребителя.

1) Сервизният инженер на Изпълнителя, предприема технически дейности по отстраняване на инцидента. В това число дистанционна намеса, ако инцидентът е на отдалечено работно място или система.
2) Ако заявката се реши на второ ниво, Сервизният инженер описва предприетите действия във формата на заявката за обслужване.
3) Сервизният инженер актуализира информацията в базата знания и приключва заявката.
4) Ако Сервизният инженер не успее да отстрани инцидента дистанционно той описва предприетите действия във формата на заявката за обслужване и предава отговорността за инцидента на Оператора на Сервизния център.
5) Операторът на Сервизния център оценява необходимостта от намеса на място и предава задачата за отстраняване на инцидента към Системен инженер намиращ се в най-близката до мястото на инцидента сервизна точка.

Намеса от Ниво 2:

1) Сервизният инженер на Изпълнителя, посещава мястото на инцидента и предприема технически дейности по отстраняване на инцидента.
2) Ако заявката се реши на ниво 2, Сервизният инженер описва предприетите действия във формата на заявката за обслужване.
3) Сервизният инженер актуализира информацията в базата знания и приключва заявката.
4) Ако Системния инженер не успее да отстрани инцидента с посещението си на място той описва предприетите действия във формата на заявката за обслужване, описва извършената диагностика и предава отговорността за инцидента на Оператора на Сервизния център.
5) Операторът на Сервизния център оценява необходимостта от намеса и предава задачата за отстраняване на инцидента към звено от системата за Трето ниво на поддръжка.

Намеса от Ниво 3:

Ескалация към трето ниво на поддръжка (Сервизна организация от по-високо ниво производителя) се извършва от специалиста на второ ниво.

При ескалация към трето ниво се избира името на организацията, към която е насочен инцидента.

Специалистът на второ ниво, работещ по случая е длъжен да отразява информацията по развитието на инцидента от трето ниво.

(1) Заявката за решаване на инцидента, заедно с информацията за извършената диагностика се подава към Център за обслужване на трета организация (производител, консултант и др.).
(2) Операторът на Сервизния център обработва получената информация от Сервизен център на производителя и я регистрира в поръчката, като записва и очакваното време за отстраняване на инцидента.
(3) Операторът на Сервизния център информира Системния инженер от Ниво 2 за очакваното време за реакция и отстраняване на инцидента и осигурява неговото присъствие на мястото на инцидента.
(4) При решение на заявката от външната организация, отговорна за поддръжката на даден продукт (напр. фирма производител на съответния продукт), представител на производителя издава документ за решена заявка.
(5) След извършването на намесата от трета страна по поддръжката Сервизният оператор информира Сервизният инженер от Ниво 2 за необходимостта от извършване на допълнителни дейности, които са необходими за възстановяване на работоспособността на системата.
(6) Сервизният инженер от Ниво 2 извършва всички необходими действия до пълното възстановяване на системата.
(7) След пълното възстановяване на работоспособността на системата Сервизният инженер описва предприетите действия във формата на заявката за обслужване.
(8) Сервизният инженер актуализира информацията в базата знания и приключва заявката.
(9) Оператор на системата попълва предприетите действия във формата на заявката и актуализира информацията в базата знания.
(10) Потребителят на системата потвърждава приключването на заявката. Ако потребителят на системата не одобри приключването на заявката то той подава по един от каналите информация до Оператора на центъра заедно с мотивите за неодобрението на приключването. В такъв случай Операторът на Сервизния център подновява дейността по отстраняването на инцидента от етап от който е необходимо да бъдат извършени допълнителните технически дейности за пълното възстановяване на системата.
(11) Ако заявката за обслужване не бъде решена от сервиза или външната организация, тя остава неприключена.
(12) На всички стъпки представителят на Възложителя получава информация съответно за решаването и закриването на заявката за обслужване или за пренасочването ѝ.
(13) При приключване на заявката, отговорник от системата за поддръжка уведомява представителя на Възложителя, подал заявката и оставя заявката в статус завършена и неприключена до окончателното одобрение от страна на представителя на Възложителя.
(14) Операторът на Сервизния център оценява развитието на работата по отстраняване на инцидента и ако инцидентът отговаря на критериите за учредяване на запис за проблем извършва регистриране на проблем. Разрешаването на проблемите е задача на процес Управление на проблемите.

След приключване на работата по разрешаване на инцидента ИТ специалистът е длъжен да отрази начина на завършване, като въведе т.н. код на затваряне. Задължително се описва цялостното решение по разрешаването на потребителската заявка или инцидент. Решението може да бъде използвано за по-нататъшна информация при възникнал проблем.

При създаването или актуализирането инцидент, съществува възможност за търсене в Базата знания за намиране на подходящо решение. При намирането на решение на проблема специалистът може да използва намереното решение и директно да затвори заявката

Настъпилата повреда и/или несъответствие се отстранява до възстановяване на пълната работоспособност на оборудването. Отстраняването на настъпила повреда и/или несъответствието се осъществява по местоположение на оборудването.

За всяка извършена дейност, свързана с гаранционната поддръжка, се изготвя и предоставя протокол, който съдържа описание на извършеното. Протоколът се подписва от представители на двете страни. На всяко тримесечие се предоставя обобщен отчет за извършените дейности по гаранционно обслужване, които се приемат от клиента. В обобщените отчети се посочва най-малко следната информация: период на покритие на отчета и списък с възникналите проблеми и параметрите, при които са отстранени проблемите. Всички разходи по време на гаранционното обслужване са за наша сметка.

Разрешаването на потребителската заявка от оператора на Сервизния център изисква извършване на поредица от действия. Преди всичко той е длъжен да прегледа и попълни коректно детайлите за заявката – описание, засегнат ИТ актив, предприети действия. При затварянето на заявката задължително се избира код на затваряне, категоризиращ начина на разрешаване на заявката. Задължително се описва решението, за да може то да бъде използвано за по-нататъшна информация при възникнал проблем.

В случаите, когато заявителят сам разреши инициирана от него потребителска заявка, то той има възможност сам да затвори заявката.

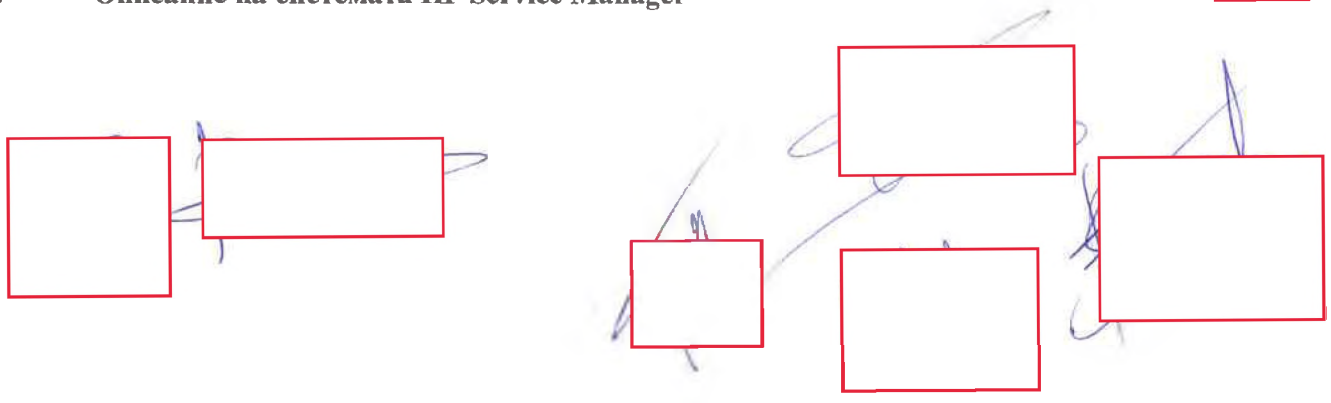
Координаторът на инциденти отговарят за навременното и качественото разрешаване на инциденти от ИТ специалистите от работната група. Той преглежда и разпределя при необходимост инциденти, насочени към работната група. Координаторът на инциденти следи за изпълнението на сроковете за разрешаване на инциденти от работната група, в зависимост от дефинираното време. Срокът за разрешаване на инцидент се определя в зависимост от приоритета на инцидента, които от своя страна се определя от степента на влияние и спешността на възникналата неработоспособност.

В случаите, в които инцидента е насочен към работна група и не е поет от лице от работната група, до 25% от времето за разрешаване, Координаторът на инциденти (ръководител на работната група) получава автоматично известие по електронната поща за предприемане на действие по възлагане на инцидента.

Ако до 75% от времето за разрешаване , инцидентът е поет от специалист и все още не е разрешен, то специалистът и мениджърът на работната група получават нотификация по имейла.

Ако крайният срок за разрешаване на инцидент е изтекъл и инцидентът все още не е разрешен, то ръководителят на работната група и специалистът получават автоматично съобщение по електронната поща.

I. Описание на системата HP Service Manager



а. Възможности на системата:

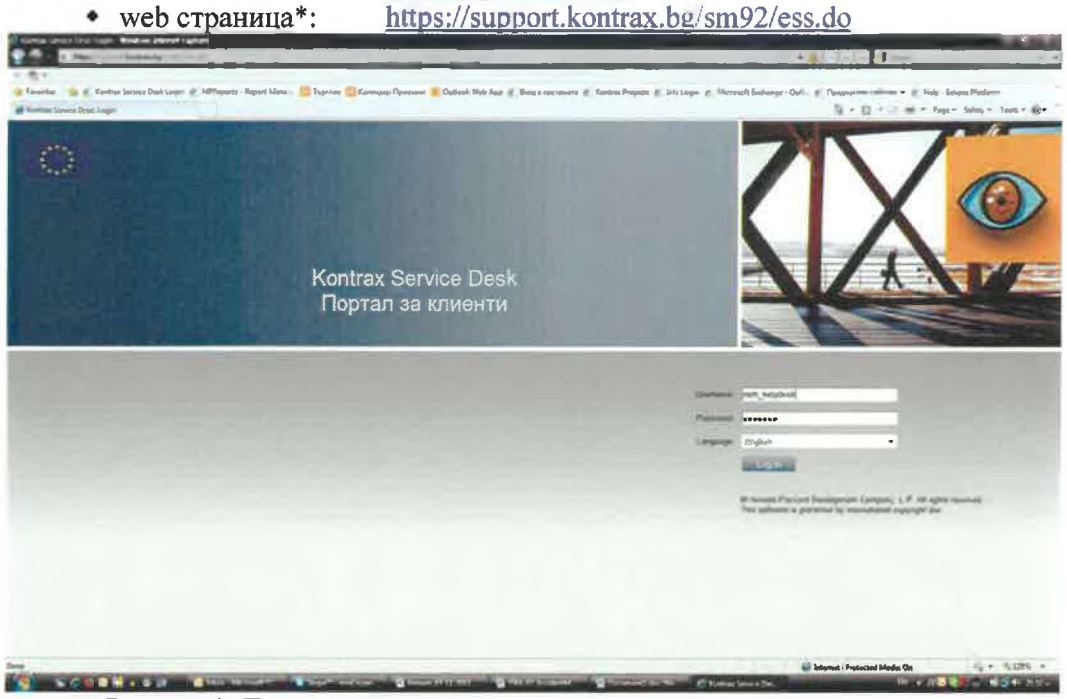
- Модулът Сервизен център (Service Desk) предоставя възможност за осъществяване на запис, наблюдение и последваща обработка на сервизни заявки и инциденти по време на целия цикъл от възникването им до тяхното решаване. Това е основният инструментариум за реализация на процеса по управление на инцидентите в процеса на обслужване.
- Процесът по Управление обхваща Сервизните заявки в Service Manager системата:
- Сервизната заявка се използва за регистриране на възникнал проблем относно обектите в ИТ инфраструктурата предмет на обслужването. Сервизна заявка се регистрира в момента на нейното получаване, след което постоянно се актуализира с информация, необходима за разрешаването на възникналия проблем.
- ИТ Service Desk (Service Desk) поддържа база от знания за начини на разрешаване на възникнали инциденти, която подпомага потребители и специалисти. Информацията, съхранена в базата ще се използва за изготвяне на справки и отчети по изпълнението на условията и параметрите на договора.
- ИТ Service Desk (Service Desk) функционира като реализира процедура при регистриране на заявка за обслужване, която представлява последователност от действия – запис в база данни, насочване към оператор, ескалация към по-високо ниво.
- HP Service Manager, чрез който се реализира ИТ Service Desk (Service Desk) позволява въвеждане на заявка за обслужване през WEB интерфейс-форма или чрез електронна поща.
- HP Service Manager съхранява всички данни от създаването и обработването на дадена заявка и предоставя възможности за детайлно докладване на проблема - в колко часа е получена заявката, от кой потребител и за какъв проблем е докладвано, кой и колко време и работил по разрешаването, времената за реакция, начинът по който е разрешена и т.н.
- HP Service Manager поддържа автоматичен контрол за срока за изпълнение на заявката и при закъснение – същият е свързан и с ескалиране на проблемните заявки по предварително дефинирана процедура.
- HP Service Manager осъществява проследяване на предприетите действия в хода на изпълнение на сервизните заявки. На базата на предварително дефинирани правила и нотификации се организира автоматично следене на настъпило събитие и уведомяване на участниците в процеса.
- HP Service Manager използва механизми за уведомяване на участниците в процеса чрез електронна поща, sms като поддържа всички удобни и надеждни методи за комуникация.
- HP Service Manager известява крайния потребител за резултатите от изпълнението на заявката чрез електронна поща, WEB портал и/или чрез други комуникационни средства. HP Service Manager е WEB базирана система и предлага следене на статуса на заявката чрез WEB-интерфейс, както за операторите, така и за крайните клиенти.
- Всички модули на ИТ Service Desk (Service Desk) съхраняват получените съобщения (reports) за проблеми в централизирана база данни (CMDB) и предприетите действия по отстраняването им. Това служи за допълване на

системата от база от знания (HP Service Manager Knowledge Mangement), която изпълнява ролята на хранилище за готови решения, които могат да се използват при възникване на проблем.

b. Регистриране на заявки

Подаването на сервизна заявка към Сервизния център (звеното за приемане на заявки за сервиз) може да бъде извършено на посочени от Контракс e-mail, web страница или телефон, а именно:

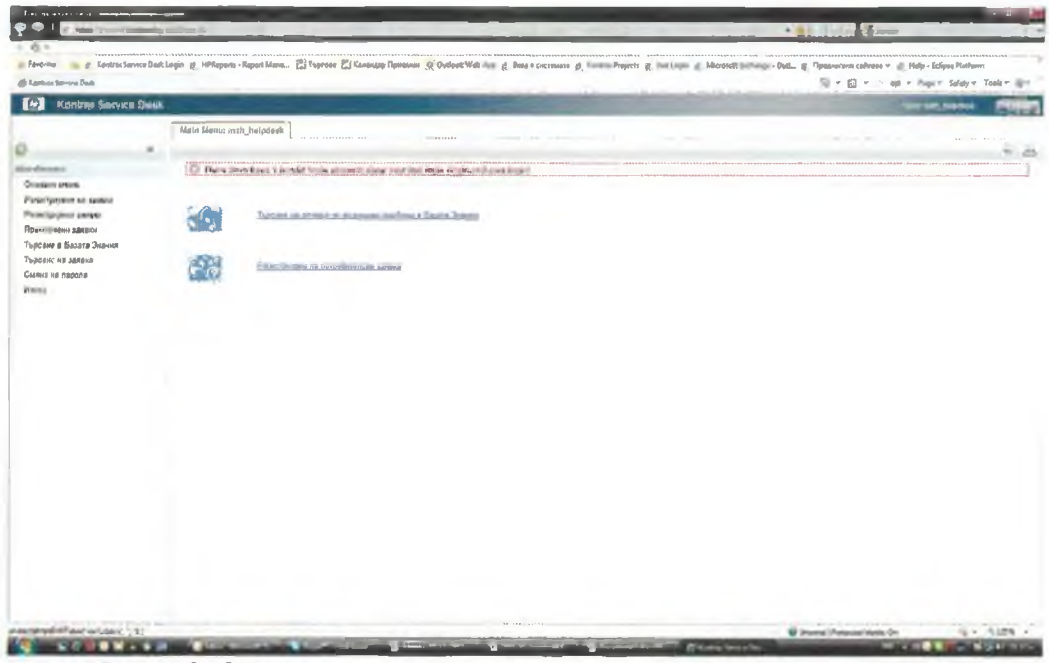
- Телефон: 9609 792 или 0700 17977
- Факс: 9609 797
- e-mail адрес: service@kontrax.bg
- web страница*: https://support.kontrax.bg/sm92/ess.do



Фигура 1: Екран за вход

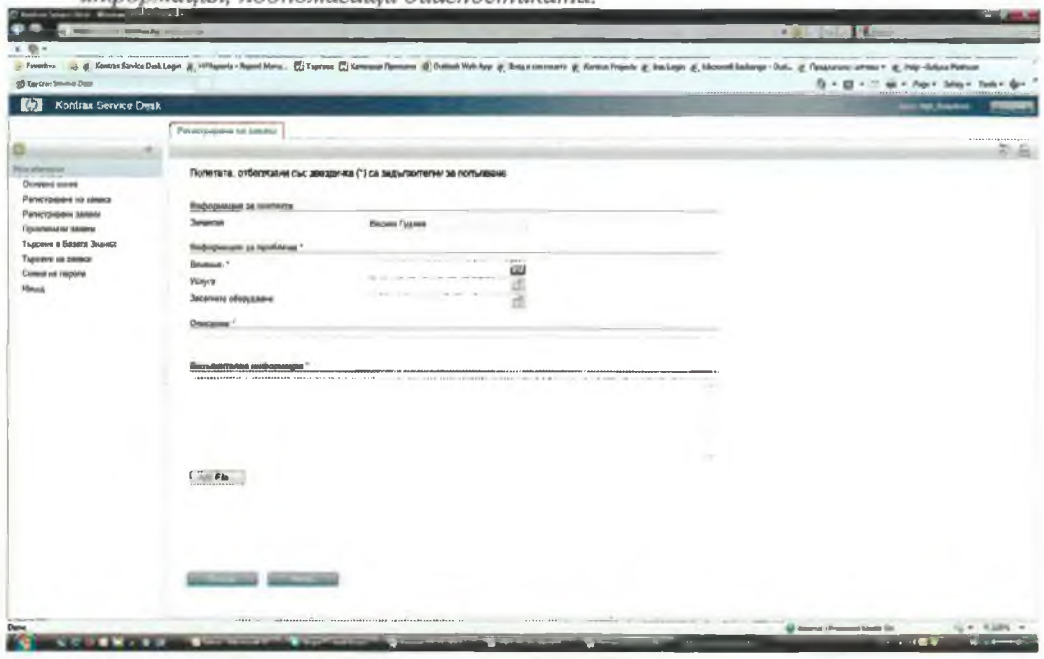
** за всеки упълномощен от Възложителя потребител Контракс създава акаунт, потребителско име и парола. Всеки потребител има следните възможности:*

Контракс АД
София 1113, ул. Тинтява 13
тел.: (02) 960 9777; факс: (02) 960 9797
e-mail: sales@kontrax.bg; www.kontrax.bg



Фигура 2: Основен екран на системата

1) подаване на заявки с възможност да избере засегнатите устройства или основните модули, които са предмет на гаранционното обслужване. При подаване на заявката потребителят може да избере устройството по сериен номер, модел, наименование на конкретен модул. Има възможност да избере влиянието, което има инцидента (повредата). Да въведе описание на повредата (инцидента), както и да приложи допълнителни файлове с информация, подпомагащи диагностиката.



Фигура 3: Екран за регистриране на заявка

2) Получаване на съобщения през електронна поща, при всяка промяна на състоянието (статуса) на поръчката: След всяко действие на Сервизния център или на сервизен инженер по дадена сервизна заявка и попълване на информацията, потребителят получава електронно съобщение (e-mail), който съдържа информация за действието и за статуса на изпълнението на заявката.

3) Мониторинг: Потребителят има възможност да проследи състоянието на всяка сервизна заявка, регистрирана от него, в това число отворени и неприключени заявки, но също така и всички приключени сервизни заявки.

4) База знания (Knowledge base): Всеки потребител има възможност да търси информация за вече идентифицирани сервизни проблеми и тяхното решение, както и за начини за решаване на проблеми и инциденти, които са предварително регистрирани в базата знания.

с. Функционална схема

HP Service Manager е WEB базирана система и предлага възможност за различен достъп (на база права на потребителите/операторите) до модула, като не е необходима инсталацията на допълнителен софтуер. HP Service Manager осъществява пълен контрол на достъпа до системата от страна на оторизираните потребители.

Системата има средства за генериране на отчети на база разрези от информационните масиви, с помощта на които Контракс ще изготвя и предоставя актуална информация за различни управленчески нива на Възложителя (за мениджъри, за оперативни звена и др.). HP Service Manager притежава средства за бързо и лесно изготвяне на отчети и статистика за приетите заявки и общия процентен дял на решените проблеми; HP Service Manager разполага и с предварително дефиниране на собствени отчети по зададени критерии с възможност за графично представяне на данните; За нуждите на договора допълнително ще бъдат разработени и статистически отчети за максимален брой на приеманите заявки за единица време и средно време за обслужване на заявките.

Правата в HP Service Manager Service Desk се дефинират на база предварителни шаблони с детайлна гранулярност до данните, което дава възможност за определени потребителски групи имат права до определени ресурси на системата, т.е. потребителите не е необходимо да имат достъп до всички ресурси.

Модулите на HP Service Desk (Service Desk) дават възможност за настройка на изгледа по групи потребители за различните нива на поддръжка.

Във връзка с наличието на т.н. „чувствителни" данни в някои заявки, HP Service Manager осигурява високо ниво на защита на информацията, а именно:

- ограничаване на достъпа на крайните потребители през WEB само до информация за собствените им заявки;
- поддържане на различни права за достъп на операторите до информацията на модулите;
- защита на информацията на модулите срещу достъп от страна на неоторизирани лица.
- Средства за одит (дневници) на всички действия.

На схемата в Приложение 1, е изложена диаграма на процеса Управление на заявките и инцидентите. Описани са ролите на отделните длъжностни лица, отговорни за процеса на обслужване.

Дефинирани са три нива на поддръжка – две вътрешни нива и трето ниво към външна сервизна организация.

Първото ниво са т.н. Оператори на Сервизен център, които поемат всички сервизни заявки. Всички заявки, касаещи ИТ инфраструктурата и ИТ услуги, задължително се регистрират, независимо от тяхната сложност. Определени от Възложителя потребители могат да регистрират заявки през web интерфейс. В изключителни случаи се използва телефонно обаждане или електронна поща.

Контракс АД
София 1113, ул. Тинтява 13
тел.: (02) 960 9777; факс: (02) 960 9797
e-mail: sales@kontrax.bg; www.kontrax.bg

Операторите регистрират заявките, определят техния приоритет и се опитват да разрешат възникналия проблем.

Ако операторът не може да разреши проблема, той го ескалира към второ ниво, към група специалисти с необходимата компетентност. Ескалацията е функционална и се извършва към работна група от специалисти. При ескалацията се регистрира инцидент, като се определя неговия приоритет и време за разрешаване.

Наличните специалисти от работната група решават кой ще поеме обработката на инцидента. Съответният специалист на второ ниво поема инцидента и започва работа по разрешаване на инцидента и регистриране на информацията във вече създадения запис от специалиста на първо ниво.

Ако до 25 % от времето за отстраняване на проблема, инцидентът не е поет за изпълнение от сервизен специалист от Работната група, системата изпраща предупредително съобщение до ръководителя на Работната група.

Ако до 75 % от времето за отстраняване проблема, Инцидентът не бъде разрешен, системата генерира автоматично предупредително съобщение до ръководителя на Работната група и до специалиста, поел инцидента.

Ако времето за отстраняване проблема е просрочено и Инцидентът не бъде разрешен, системата генерира автоматично предупредително съобщение до ръководителя на Работната група и до специалиста, поел инцидента.

При затваряне на инцидента, съответната потребителска заявка се затваря автоматично.

Когато не е насочена към правилната работна група, то инцидентът се връща обратно към оператора от Сервизния център, който го е регистрирал. При такъв вид действие, специалистът на второ ниво е длъжен да опише защо счита, че случаят не е от компетентността на неговата група.

Ескалация за трето ниво (напр. производители) се извършва от специалиста на второ ниво. Специалистът на второ ниво работещ по случая е длъжен да отразява информацията по развитието на инцидента от 3-тото ниво. Третото ниво включва сервизни организации от високо ниво на производителя, които нямат достъп до системата.

Дата: 13.07.2020 г.

Печат и подпис: .....

Николай Йорданов
/име и фамилия/

КОНТРАКС АД 1

ПАПКА

„ПРЕДЛАГАНИ ЦЕНОВИ ПАРАМЕТРИ“

по

обособена позиция № 7 с предмет: „Доставка на система за защита от изтичане/загуба на данни от крайните точки и от мрежата“

от

Контракс АД

Контракс АД
Гр. София 1113
Ул. „Тинтява“ № 13
Тел: 02/9609777, факс: 02/9609797
tenders@kontrax.bg

Заличаванията на информация в документа са на основание чл. 4 от Общ регламент за защита на данните

ПРИЛОЖЕНИЕ № 3.7

ДО
„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД
ГР. СОФИЯ, УЛИЦА „ПАНАЙОТ ВОЛОВ“ № 2

ЦЕНОВО ПРЕДЛОЖЕНИЕ

Наименование на обществената поръчка:	***„Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите“***
Наименование на обособена позиция, за която участникът подава оферта	***Обособена позиция № 7: „Доставка на система за защита от изтичане/загуба на данни от крайните точки и от мрежата“***
Наименование на участника:	***КОНТРАКС АД***
Правно-организационна форма на участника:	***Акционерно дружество*** *(физическо или юридическо лице, обединение или друго образувание, което има право да изпълнява доставки съгласно законодателството на държавата, в която е установено)*
Седалище по регистрация и адрес на управление:	**Град София, 1113, ул. „Тинтява“ №13**
ЕИК / Код по регистър БУЛСТАТ/ регистрационен номер или друг идентификационен код:	**175415627**
Представляващ	**Николай Йорданов – Изпълнителен директор** *(законен представител или лице, специално упълномощено за участие в процедурата[1])*

УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА,

След запознаване с документацията за участие в обществената поръчка с горепосочения предме
ние предоставяме следното ценово предложение по горецитираната обособена позиция:

[1] Съгласно чл. 41, ал. 5 от Правилника за прилагане на Закона за обществените поръчки (ППЗОП) когато документи, свързан
с участие в обществени поръчки се подават от лице, което представя участника по пълномощие, в Единния европейск
документ за обществени поръчки (ЕЕДОП) се посочва информация относно обхвата на представителната му власт

Заличаванията на информация в документа са на основание чл. 4 от Общ регламент за
защита на данните

1. Предлагаме да изпълним доставката, предмет на горецитираната процедура за възлагане на обществена поръчка при цени, както следва:

№	Описание	Количество	Единична цена в лв. без ДДС	Обща цена в лв. без ДДС
I.	II.	III.	IV.	V.
1.	Платформа за защита от изтичане/загуба на данни от крайните точки и от мрежата	1 бр.	1 684 045.00	1 684 045.00

2. В цената по т. 1 са включени всички разходи за изпълнение на поръчката. Потвърждаваме, че възложителят няма да дължи заплащането на каквито и да е други разноски, направени от нас като изпълнител.

3. Потвърждаваме, че цената по т. 1 е постоянна за целия срок на договора и не подлежи на промяна за времето на изпълнение на договора, освен в случаите когато това е в полза на възложителя.

Приложения: Количествено-стойностна сметка

Забележка:

1. *Предложените от участника цени следва да са в български лева без ДДС, закръглени до втория знак на десетичната запетая.*

2. *Участник, който допусне аритметична грешка, се отстранява от участие в процедурата по съответната обособена позиция.*

3. *Участник, който предложи обща цена, която е по-висока от прогнозната стойност на съответната обособена позиция, се отстранява от по-нататъшно участие в процедурата по съответната обособена позиция.*

4. *Липсата на ценово предложение, както и предоставянето на ценово предложение, което не отговаря на изискванията на документацията за обществената поръчка, е основание за отстраняване от по-нататъшно участие в процедурата по съответната обособена позиция.*

Дата на подписване: 13/ 07/ 2020 г.

Подпис и печат: .....

Име и фамилия Николай Йорданов

Длъжност Изпълнителен директор

Наименование на участника Контракс АД

КОНТРАКС АД 1

ПРИЛОЖЕНИЕ

към Ценово предложение

от фирма КОНТРАКС АД

по *Обособена позиция № 7: „Доставка на система за защита от изтичане/загуба на данни от крайните точки и от мрежата“*

КОЛИЧЕСТВЕНО-СТОЙНОСТНА СМЕТКА

Платформа за защита от изтичане/загуба на данни от крайните точки и от мрежата

№	Описание	Продуктов №	Бр.	Единична цена в лв. без ДДС	Обща цена в лв. без ДДС
1	Лицензионен абонамент за платформа за защита от изтичане/загуба на данни от крайните точки и от мрежата Forcepoint DLP Suite (IP Protection), User & Data Security за 60 месеца	DLPSIP-4-CP60-X-N	8000	175.42	1 403 360.00
2	Подсилено ниво на поддръжка Enhanced Support за Forcepoint DLP Suite (IP Protection), за 8000 потребителя, за 60 месеца	ENHSPT-4-CP60-X-N	1	280 685.00	280 685.00
				Обща цена в лв. без ДДС:	**1 684 045.00**

13.07.2020 г.

Подпис и печат:

Николай Иорданов,

Изпълнителен директор

КОНТРАКС АД 1