ИНФОРМАЦИОННО ОБСЛУЖВАНЕ
1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340, ЕИК: 831641791
office@is-bg.net www.is-bg.net

ПОКАНА

„Информационно обслужване" АД, със седалище и адрес на управление: гр. София, ул. „Панайот Волов" № 2, тел. 02/9420340, e-mail: office@is-bg.net, представлявано от **Ивайло Филипов – Изпълнителен директор**, Ви кани да участвате в процедура за избор на доставчик, при следните условия:

1. **Предмет на процедурата:**

„Закупуване на защитни стени за дейта център за нуждите на „Информационно обслужване" АД".

Количествената и техническа спецификация на защитните стени е посочена в Техническо задание – Приложение №1.

2. **Срок за изпълнение:**

2.1. Срок за доставка на 2 (два) броя устройства - до 30 дни, считано от датата на сключване на договор.

2.2. Срок на софтуерна и хардуерна гаранционна поддръжка – минимум 36 месеца, считано от датата на приемо-предавателния протокол за доставка.

3. **Критерии за оценка на предложенията:** „най-ниска предложена цена".

Участниците се класират според предложената от тях обща цена в лева без ДДС. На първо място се класира участникът, предложил най-ниска цена. Оценката на предложенията се извършва съгласно Методика за оценка на предложенията, приложена към настоящата покана (Приложение № 2).

4. **Списък на документите, които кандидатите следва да представят:**

4.1. Документи за идентификация и квалификация:

4.1.1. Поименно оторизационно писмо от производителя на предложеното решение или от негов официален представител за територията на Република България за участие в конкретната процедура, издадено след датата на публикуване на настоящата процедура.

4.1.2. Декларация по образец – Приложение № 5.

4.2. Техническо предложение, изготвено по образец - Приложение № 3.

4.3. Ценово предложение, изготвено по образец - Приложение № 4.

5. Начин на плащане: извършва се по банков път, в срок до 30 (тридесет) дни след подписване на приемо-предавателен протокол, удостоверяващ извършването на доставката без възражения и забележки от страна на Възложителя и издадена фактура от Изпълнителя

1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340, ЕИК: 831641791
office@is-bg.net www.is-bg.net

6. **Максимална обща цена** – кандидатите следва да предложат цена, която не надвишава определената максимална обща цена от **325 000 (триста двадесет и пет хиляди) лв. без ДДС**.

   Кандидат, предложил по-висока от максималната обща цена, ще бъде отстранен от участие в процедурата.

7. **Срок на валидност на предложението** - срокът на валидност да бъде не по-малко от 60 (шестдесет) календарни дни, считано от датата на представяне на предложението.

8. **Подаване на предложението:**

8.1. Срок, място и начин:

Предложението следва да бъде подадено по електронен път в срок **до 12:00 часа на 27.06.2024 г.**, на следния адрес на електронна поща: office@is-bg.net.

8.2. Изисквания към подаване на предложението:

Техническото предложение (Приложение № 3), Ценовото предложение (Приложение № 4) и Декларацията (Приложение № 5) се съставят като електронни документи във формат .pdf и се подписват с квалифициран електронен подпис.

Ако към предложението е необходимо да бъде представен документ, който е издаден на хартиен носител, същият се представя сканиран и заверен с квалифициран електронен подпис.

В случай, че обстоятелства от документите за идентификация и квалификация са достъпни чрез публичен безплатен регистър или информацията е публично достъпна на друг официален адрес, кандидатите могат да посочат електронен адрес, на който тази информация е налична и достъпна.

Електронното съобщение, с което се подава предложението в настоящата процедура, следва да съдържа данни за:

1. наименованието на участника;
2. телефон и електронен адрес;
3. наименованието на процедурата, за която се подават документите.

За дата и час на получаване на предложението се приемат датата и часа на получаване на предложението на посочения в т. 8.1 адрес на електронна поща за подаване на предложения.

„Информационно обслужване“ АД използва инструменти за осигуряване на сигурността на информацията, предавана по електронна поща, които могат да забавят получаването на електронни съобщения, поради което е препоръчително предложенията в настоящата процедура да се изпращат най-малко 30 минути преди крайния срок по т. 8.1.

9. **Лице за контакти с „Информационно обслужване” АД**

Георги Костадинов, ръководител, информационни и комуникационни технологии, отдел „Системна интеграция“, мобилен: +359 876 548 419, e-mail: g.kostadinov@is-bg.net.

10. **Участници в процедурата**

В процедурата могат да участват и кандидати, до които не е изпратена изрична покана.

ИНФОРМАЦИОННО ОБСЛУЖВАНЕ
1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340, ЕИК: 831641791
office@is-bg.net www.is-bg.net

11. Приложения:

11.1. Техническо задание – Приложение № 1;
11.2. Методика за оценка на предложенията – Приложение № 2;
11.3. Техническо предложение – образец - Приложение № 3;
11.4. Ценово предложение – образец - Приложение № 4;
11.5. Декларация – образец – Приложение № 5;
11.6. Указания за участие в процедурата – Приложение № 6.

Digitally signed by
Ivaylo Borisov Filipov
Date: 2024.06.19
13:48:02 +03'00'

ИВАЙЛО ФИЛИПОВ
ИЗПЪЛНИТЕЛЕН ДИРЕКТОР
„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ” АД

Приложение № 1

ТЕХНИЧЕСКО ЗАДАНИЕ

с

Количествена и техническа спецификация за закупуване на
защитни стени за дейта център за нуждите на „Информационно обслужване“ АД

Количество – 2 броя

1. Функционални изисквания на системата:

1.1. Изграждане на сектори с различна степен на доверие, които да разделят мрежата на отделни сегменти и прилагане на политики на база потребителски имена от Активната Директория;

1.2. Системата да анализира съдържанието за наличие на зловреден код като включва минимум AntiVirus, AntiSpyware, IPS;

1.3. Системата да има възможност чрез допълнителен лиценз да анализира непознати заплахи (Zero Day зловреден код) в защитена среда като създава и дистрибутира сигнатури в реално време.

1.4. Системата за IPS да използва машинно, задълбочено обучение да открива и блокира непознати Command and Control (C2) като Empire и Cobalt Strike Command and Control при преминаване на непознат HTTP, HTTP2, SSL, TCP и UDP трафика през защитната стена.

1.5. Системата за анализ на Zero Day зловреден код трябва да използва минимум следните методи за анализ: Static Analysis, Machine Learning, Dynamic Analysis

1.6. Системата да има възможност чрез допълнителен лиценз да анализира PE и PowerShell скриптове в защитната стена и предоставя защита в реално време.

1.7. Системата следва да инспектира за заплахи HTTPS протокола чрез декриптиране;

1.8. Системата следва да инспектира за заплахи HTTP 1.1 и HTTP 2.0 протоколи;

1.9. Да има възможност чрез допълнителен лиценз да филтрира уеб сайтовете по категории и ограничаване на достъпа до опасно съдържание в Интернет, включително мултикатегоризация на URL съгласно тип на съдържанието и риск;

1.10. Системата да има възможност чрез допълнителен лиценз да анализира URL и тяхното съдържание в реално време. Всяка заявка за достъп да бъде анализирана чрез Machine Learning на база на HTTP Request.

1.11. Управлението на устройството трябва да се реализира чрез физически отделени процесор, памет и интерфейси отделени от ресурсите използвани за управление на трафика.

1.12. Решението да може да дистрибутира входящите NAT сесии между няколко адреса като използва минимум следните методи : Round Robin, Source IP Hash, Least Sessions

1.13. Администратора трябва да може да изисква прекатегоризация на даден URL директно от графични интерфейс на защитната стена.

1.14. Решението да има възможност чрез допълнителен лиценз да използва вътрешните ресурси на защитната стена за да анализира и открива зловреден JavaScript код и кражба на корпоративни потребителски имена и пароли чрез Phishing.

1.15. Наличие на DLP (Data Loss Prevention) функционалност, за ограничаване на движението на конфиденциални файлове.

1.16. Политиката за декриптиране трябва да има възможност да се настройва на база на URL или URL категория;

1.17. Решението да притежава възможност да ограничава достъпа на потребителите до Web сървъри, които не поддържа минимални изисквания за валиден публичен сертификат и съответно високо ниво на сигурност (TLSv1.1, TLSv1.2, TLSv1.3);
1.18. Препращане на подозрителните DNS заявки към устройството с цел ограничаване на достъпа и регистриране на заразени машини в мрежата;
1.19. Предложението решение трябва може да изгражда отдалечен VPN достъп чрез агент инсталиран на крайно клиентската машина с Windows и Mac OS .
1.20. След добавяне на лиценз агента за VPN достъп трябва да поддържа (да може да бъде инсталиран) минимум следните операционни системи: Linux, Android, iOS, Raspbian, Ubunto.
1.21. Възможност за QoS трафика според типа приложение потребител и/или URL категория;
1.22. Прозрачна идентификация на потребителите от Активната директория без изискване на крайната машина да се инсталира агент, настройки в browser или отваряне на Web Portal;
1.23. Решението да може да изпраща декриптирани потоци от данни към трети страни за допълнителен анализ след което отново да криптира трафика.
1.24. Да предоставя възможност за надграждане с допълнителен лиценз за идентифициране на устройства (Device Fingerprint) в мрежата на база поведение, мета данни и логове. За карантина на заразени устройства независимо от техните IP адреси, локация и потребител.
1.25. Да предоставя възможност за надграждане с допълнителен лиценз за съставяне на политика за сигурност базирана на устройство независимо от неговия IP Address, локация и потребител.
1.26. Решението да може да чете данните в X-Forwarded-For (XFF) за идентифициране на реалния източник на данни (IP Address), когато той се намира зад други мрежови устройства.
1.27. Защита на корпоративните потребителски имена и пароли, посредством блокиране или ограничаване на тяхното използване в външни за организацията системи и публично достъпни доставчици (Dropbox, Google, Facebook, LinkedIn).
1.28. Решението да включва функционалност позволяваща служебния достъп до публични облачни услуги като Office 365, Google, Dropbox и YouTube, и ограничаваща достъпа до лични потребителски акаунти за същите приложения.
1.29. Анализа на логовете и репортинг да се извършва от самото устройство с през неговия графичен интерфейс без да необходима инсталация на допълнителен софтуер;
1.30. Решението да притежава Уеб базиран интерфейс с различни статистики на база време, приложение, категории, потребители, заплахи и други;
1.31. Генерираните отчети и логове следва да са обогатени с данни за потребител и група, получена от интеграция с бази за управление на потребителите (Active Directory, LDAP и други);
1.32. Решението да може автоматично да тегли IP, Domain или URL листи от Web Server собственост на Възложителя или външна организация с цел ограничаване / позволяване на достъпа до горе споменатите.
1.33. Решението да може автоматично да открива какви приложения работят в организацията и да предлага лист от такива, които да бъдат добавени към нови или вече съществуващи правила за сигурност.
1.34. Решението да притежава облачна услуга за събиране и анализ на служебни данни от устройството като чрез машинно обучение препоръчва добри практики и открива аномалии в нормалната работа.
1.35. Да има възможност за надграждане чрез лиценз за услуга която позволява на защитната стена да категоризира непознати приложения в облака на производителя за които няма конкретни предварително дефинирани сигнатури.
1.36. Системата да може да пропуска до три софтуерни версии при upgrade или downgrade

1.37. Решението да предоставя възможност за надграждане чрез лиценз за защита на крайно клиентските машини, позволяващ събиране и анализ на всички логове (от крайните точки и защитните стени) в защитена облачна среда на производителя;
1.38. Решението да има възможност чрез допълнителен лиценз, механизъм за откриване и превенция на DNS Tunneling канали за комуникация, включително възможност да следи и ограничаване достъпа до автоматично генерирани домейни (Domain generation algorithms (DGA));
1.39. Системата да има възможност за надграждане с допълнителен лиценз за отдалечен защитен достъп от телефони и таблети (с операционни системи iOS, Android) и инспекция (compliance check) на крайно клиентската машина, който се извършва по време на изграждането на защитена връзка;
1.40. Системата да има възможност за надграждане с допълнителен лиценз инсталиран на защитната стена, с който да открива и управлява IoT (Internet of Things) устройства като предоставя възможност за автоматично генериране на препоръчани правила за достъп и контрол.

2. Технически параметри:

Всеки Участник следва да предложи 2 (две) устройства с еднакви параметри – модел, версия на Firmware, настройки и спецификация за осигуряване на непрекъсваемост на мрежовата услуга. Устройствата следва да бъдат конфигурирани и да работят в High Availability режим (active-passive), като всяко от тях отговаря на следните технически параметри:

Параметър	Минимално изискване
Минимална пропускателна способност с активирана функция за идентификация на приложенията	50.0 Gbps
Минимална пропускателна способност с активирани всички функционалности за защита: IPS/ AntiVirus/ Anti-Malware / URL / Firewall / Application Control	33 Gbps
Минимална производителност за IPsec VPN	20 Gbps
Минимален брой TCP сесии	4 500 000
Минимален брой нови сесии в секунда	265 000
Разпознати и поддържани приложения (минимум)	4 300
Минимален брой мрежови интерфейси	Да разполага 8 X 1G/2.5G/5G/10G Base-T ports Да разполага с възможност за надграждане с допълнителни минимум 12 x 10Gbit/s SFP+ 4 x 40G/100Gbit/s QSFP+/QSFP28 4 x 25Gbit/s SFP28
Режими на работа на интерфейсите	L2, L3, Tap, Transparent едновременно/микс да се използват върху едно устройство.
Машрутизиращи протоколи	OSPFv2/v3, BGP with graceful restart, RIP, static routing Policy-based forwarding Point-to-Point Protocol over Ethernet (PPPoE) Bidirectional Forwarding Detection (BFD)
Минимални изисквания към IPSec имплементация	Key exchange: manual key, IKEv1 and IKEv2 (pre-shared key, certificate authentication)

	Encryption: 3DES, AES (128-bit, 192-bit, 256-bit) Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512 Post-quantum VPN : quantum-resistant IKEv2 VPNs based on the RFC 8784
Минимален брой конкурентни SSL VPN потребителя включени в системата (постоянни лицензи)	15 000 SSL VPN потребителя
Минимален брой IPSec Site-to-Site VPN	10 000 отдалечени точки
Устройството да поддържа виртуални таблици за маршрутизация	минимум 20 броя
Устройството да има възможност да поддържа виртуализация (виртуални контексти)	10 броя
IPv6 поддръжка	Всички конфигурации за интерфейсните модули на защитната стена трябва да поддържат IPv6 както и всички контролни функции на системата трябва да се налични и за IPv6
Инспекция на SSL криптиран трафик, без оглед на прилежащия протокол, като предоставя декриптирания трафик на всички свои функционални компоненти, за инспекция и налагане на политики над съдържанието	Системата следва да декриптира и инспектира SSL като поддържа TLS v1.1, TLS v1.2, TLS v1.3
Управление на устройството	Всяко от устройствата в системата да има възможност да се управлява посредством имплементация на REST based API, извличане на данни и репорти в XML формати. Всяко от устройствата в системата следва да поддържа всеки един от следните методи за управление: CLI, уеб конзола, централизирана система за управление
Режим на надеждност	Active-Passive, Active/Active Клъстер до 8 устройства разпределени в отдалечени центрове за данни
Минимален брой интерфейси за управление	1 x 1Gbit/s SFP out-of-band management port 2 x 10G SFP+ интерфейси за отказоустойчивост 1 x RJ-45 конзолен порт 1 x Micro USB Възможност за надграждане 1x40Gbit/s QSFP+ интерфейси за отказоустойчивост
Монтаж и размери	Предназначена за вграждане в 19“ шкаф с максимален размер 2U
Захранване и входно напрежение (Входяща честота)	Резервирано, 100-240VAC (50-60Hz)
Софтуерна и хардуерна гаранционна поддръжка 365x24x7	мин. 36 месеца. Участника следва да използва необходимите лицензи за гаранционна поддръжка от Производителя. Доказва се чрез посочване на партиден номер.

Допълнителни изисквания:

2.1. Всеки участник предлага клъстер съставен от 2 (два) броя устройства, като посочва марка, модел, партиден номер и линк към страницата на производителя;
2.2. За всеки технически параметър следва да се предложи детайлно описание, включително и референция към документ да производителя на предлаганото оборудване;
2.3. Всеки участник следва да е оторизиран за продажба на продукти/услуги от Производителя на предложеното решение или от негов официален представител за територията на Република България. Доказва се чрез представяне на поименно оторизационно писмо за участие в конкретната процедура, издадено след датата на публикуване на настоящата процедура;
2.4. Използваните устройства следва да са нови, неупотребявани, нерециклирани и да бъдат налични в актуалната производствена листа на техния производител.

Приложение № 2

Методика за оценка на предложенията,

подадени в процедура за избор на доставчик с предмет:

„Закупуване на защитни стени за дейта център за нуждите на „Информационно обслужване“ АД“

1. Предложенията се оценяват за съответствие с техническите изисквания в Техническото задание - Приложение № 1.

2. Предложенията, отговарящи на изискванията по т. 1, се оценяват по критерия „най-ниска предложена цена“, като се сравнява предложената обща цена в лева без ДДС.

3. На първо място се класира участникът, предложил най-ниска цена, като участниците се подреждат по възходящ ред.

Приложение № 3

Образец

ДО

„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД

УЛ. „ПАНАЙОТ ВОЛОВ“ № 2

ГР. СОФИЯ

[наименование на участника],
представлявано от [трите имена] в качеството на [длъжност, или друго качество]
с ЕИК […], със седалище […] и адрес на управление […],
адрес за кореспонденция: […],
банкови сметки: […]

ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ

за

участие в процедура за избор на доставчик с предмет:

„Закупуване на защитни стени за дейта център за нуждите на „Информационно обслужване“ АД“

След запознаване с поканата за участие в процедура за избор на доставчик с предмет: „Закупуване на защитни стени за дейта център за нуждите на „Информационно обслужване“ АД“, с настоящото Техническо предложение правим следните обвързващи предложения:

1. Срок за изпълнение:

1.1. Декларираме, че ще доставим 2 (два) броя. устройства в срок до ……...…../……/ дни (*не повече от …… дни*), считано от датата на сключване на договор.

1.2. Срокът на софтуерна и хардуерна гаранционна поддръжка е …….. – минимум 36 месеца, считано от датата на приемо-предавателния протокол за доставка.

2. Приемаме да изпълним предмета на процедурата, съгласно всички условия и изисквания, посочени от Възложителя в поканата за участие в настоящата процедура и Техническото задание - Приложение № 1.

3. Предложението е със срок на валидност …….. / ……/ календарни дни *(не по-малко от 60 /шестдесет/ календарни дни)*, считано от датата на представяне на предложението.

4. Приемаме да доставим 2 (две) устройства с еднакви параметри – модел, версия на Firmware, настройки и спецификация за осигуряване на непрекъсваемост на мрежовата услуга. Устройствата следва да бъдат конфигурирани и да работят в High Availability режим (active-passive), като всяко от тях отговаря на следните технически параметри:

Параметър	Минимално изискване
Минимална пропускателна способност с активирана функция за идентификация на приложенията	50.0 Gbps
Минимална пропускателна способност с активирани всички функционалности за защита: IPS/ AntiVirus/ Anti-Malware / URL / Firewall / Application Control	33 Gbps
Минимална производителност за IPsec VPN	20 Gbps
Минимален брой TCP сесии	4 500 000
Минимален брой нови сесии в секунда	265 000
Разпознати и поддържани приложения (минимум)	4 300
Минимален брой мрежови интерфейси	Да разполага 8 X 1G/2.5G/5G/10G Base-T ports Да разполага с възможност за надграждане с допълнителни минимум 12 x 10Gbit/s SFP+ 4 x 40G/100Gbit/s QSFP+/QSFP28 4 x 25Gbit/s SFP28
Режими на работа на интерфейсите	L2, L3, Tap, Transparent едновременно/микс да се използват върху едно устройство.
Машрутизиращи протоколи	OSPFv2/v3, BGP with graceful restart, RIP, static routing Policy-based forwarding Point-to-Point Protocol over Ethernet (PPPoE) Bidirectional Forwarding Detection (BFD)
Минимални изисквания към IPSec имплементация	Key exchange: manual key, IKEv1 and IKEv2 (pre-shared key, certificate authentication) Encryption: 3DES, AES (128-bit, 192-bit, 256-bit) Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512 Post-quantum VPN : quantum-resistant IKEv2 VPNs based on the RFC 8784
Минимален брой конкурентни SSL VPN потребителя включени в системата (постоянни лицензи)	15 000 SSL VPN потребителя
Минимален брой IPSec Site-to-Site VPN	10 000 отдалечени точки
Устройството да поддържа виртуални таблици за маршрутизация	минимум 20 броя

Устройството да има възможност да поддържа виртуализация (виртуални контексти)	10 броя
IPv6 поддръжка	Всички конфигурации за интерфейсните модули на защитната стена трябва да поддържат IPv6 както и всички контролни функции на системата трябва да се налични и за IPv6
Инспекция на SSL криптиран трафик, без оглед на прилежащия протокол, като предоставя декриптирания трафик на всички свои функционални компоненти, за инспекция и налагане на политики над съдържанието	Системата следва да декриптира и инспектира SSL като поддържа TLS v1.1, TLS v1.2, TLS v1.3
Управление на устройството	Всяко от устройствата в системата да има възможност да се управлява посредством имплементация на REST based API, извличане на данни и репорти в XML формати. Всяко от устройствата в системата следва да поддържа всеки един от следните методи за управление: CLI, уеб конзола, централизирана система за управление
Режим на надеждност	Active-Passive, Active/Active Клъстер до 8 устройства разпределени в отдалечени центрове за данни
Минимален брой интерфейси за управление	1 x 1Gbit/s SFP out-of-band management port 2 x 10G SFP+ интерфейси за отказоустойчивост 1 x RJ-45 конзолен порт 1 x Micro USB Възможност за надграждане 1x40Gbit/s QSFP+ интерфейси за отказоустойчивост
Монтаж и размери	Предназначена за вграждане в 19‘‘ шкаф с максимален размер 2U
Захранване и входно напрежение (Входяща честота)	Резервирано, 100-240VAC (50-60Hz)
Софтуерна и хардуерна гаранционна поддръжка 365x24x7	мин. 36 месеца. Участника следва да използва необходимите лицензи за гаранционна поддръжка от Производителя. Доказва се чрез посочване на партиден номер.

- **<u>Устройствата да отговарят на допълнителните функционални изисквания, посочени в техническата спецификация</u>**

ПОДПИС

[име и фамилия]

[качество на представляващия участника]

Забележка: *Техническото предложение се представя в електронен вид във формат .pdf, подписано с квалифициран електронен подпис.*

Приложение № 4

Образец

ДО

„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД

УЛ. „ПАНАЙОТ ВОЛОВ” № 2

ГР. СОФИЯ

[наименование на участника],
представлявано от [трите имена] в качеството на [длъжност, или друго качество]
с ЕИК […], със седалище […] и адрес на управление […],
адрес за кореспонденция: […],
банкови сметки: […]

ЦЕНОВО ПРЕДЛОЖЕНИЕ
за
участие в процедура за избор на доставчик с предмет:

„Закупуване на защитни стени за дейта център за нуждите на „Информационно обслужване“ АД

След запознаване с поканата за участие в процедура за избор на доставчик с предмет: „Закупуване на защитни стени за дейта център за нуждите на „Информационно обслужване“ АД и Техническото задание на Възложителя, ние предоставяме следното Ценово предложение:

1. Предлагаме да доставим защитните стени, предмет на горецитираната процедура, в съответствие с Техническото задание на Възложителя – Приложение № 1 и представеното от нас Техническо предложение – Приложение № 3 **при обща цена в размер ……..…….. (словом: ……..) лева без ДДС** и единична цена …… (……..) лева без ДДС.

2. Декларираме, че в предложената цена са включени всички разходи за изпълнение на дейностите, предмет на процедурата, включени в Техническото задание на Възложителя и представеното от нас Техническо предложение.

3. Начин на плащане – извършва се по банков път, в срок до ……../не по-малко от 30 дни/ след подписване на приемо-предавателен протокол, удостоверяващ извършването на доставката без възражения и забележки от страна на Възложителя и издадена фактура от Изпълнителя

[дата]

ПОДПИС
[име и фамилия]
[качество на представляващия участника]

Забележка: *Ценовото предложение се представя в електронен вид във формат .pdf, подписано с квалифициран електронен подпис.*

Приложение № 5

Образец

ДЕКЛАРАЦИЯ

От.....,

представляващ ..... – кандидат в процедура с предмет: „Закупуване на защитни стени за дейта център за нуждите на „Информационно обслужване“ АД**“**, в качеството ми на .....,

ДЕКЛАРИРАМ, че представляваното от мен дружество:

1. Не е обявено в несъстоятелност и не е в производство за обявяване в несъстоятелност;
2. Не е в производство по ликвидация.

ДЕКЛАРИРАМ, че:

3. Не съм лишен от правото да упражнявам търговска дейност;
4. Не съм осъден с влязла в сила присъда за престъпление против финансовата, данъчната или осигурителната система, включително изпиране на пари, по чл. 253 – 260 от НК, за подкуп по чл. 301 – 307 от НК, участие в организирана престъпна група по чл. 321 и чл. 321а от НК, както и за престъпление против собствеността по чл. 194 – 217 от НК или против стопанството по чл. 219 – 252 от НК.

ДЕКЛАРАТОР:

Забележки:

1. Декларацията се представя в електронен вид във формат .pdf, подписана с квалифициран електронен подпис.

2. Декларацията се подписва задължително от управляващия и представляващ дружеството. Когато управляващите дружеството са повече от едно лице, декларацията се подписва от всички лица, вписани в Търговския регистър като представляващи и се представя в отделен екземпляр за всяко представляващо лице.

Приложение № 6

УКАЗАНИЯ

за участие в процедура за избор на доставчик с предмет:

„Закупуване на защитни стени за дейта център за нуждите на „Информационно обслужване“ АД“

1. Кандидатите изготвят и окомплектоват предложенията си съгласно изискванията, посочени в поканата и приложенията към нея.
2. Не по-късно от 11:00 ч. на 25.06.2024 г. всеки кандидат може да поиска от Възложителя писмено разяснения по документацията. Възложителят изпраща разяснението до всички кандидати, които са получили документация за участие и са посочили адрес за кореспонденция и го публикува на интернет-страницата на „Информационно обслужване” АД.
3. Предложенията се приемат по начина и в срока, посочени в поканата. Приемат се и предложения на кандидати, които не са поканени с изрична покана.
4. Предложение, получено след изтичане на крайния срок, не се разглежда от Възложителя. В този случай до кандидата се изпраща уведомление.
5. Изборът на доставчици се извършва въз основа на подадените предложения.
6. Изпълнителният директор на „Информационно обслужване” АД назначава комисия за разглеждането и оценяването на подадените предложения.
7. Комисията отстранява от процедурата кандидат, който:
   - е обявен в несъстоятелност/ е в производство по ликвидация / е лишен от правото да упражнява търговска дейност / е осъден с влязла в сила присъда за престъпление против финансовата, данъчната или осигурителната система, за престъпление по служба или за подкуп, както и за престъпление против собствеността или против стопанството, освен ако не е реабилитиран.
   - управител или член на управителните органи на кандидат, а в случай, че членове са юридически лица – за техните представители в съответния управителен орган е лишен от правото да упражнява търговска дейност / е осъден с влязла в сила присъда за престъпление против финансовата, данъчната или осигурителната система, за престъпление по служба или за подкуп, както и за престъпление против собствеността или против стопанството, освен ако не е реабилитиран.
   - не е изготвил и окомплектовал предложението си съгласно изискванията, посочени в документацията за участие;
   - е представил непълно техническо или ценово предложение.
8. Възложителят може да изиска от кандидатите да представят допълнително документи, с които да докажат икономическото и финансовото си състояние, техническите възможности и/или квалификацията им.
9. След разглеждане на получените предложения, Възложителят може еднократно да поиска от кандидатите да представят подобрено ценово предложение.

10. Кандидатите са длъжни в процеса на провеждане на процедурата да уведомяват за всички настъпили промени в обстоятелствата, за които са представили декларация по образец (Приложение № 5 към поканата) - в 7-дневен срок от узнаването им.
11. Лице, което е дало съгласие и фигурира като подизпълнител в офертата на друг кандидат, не може да представя самостоятелна оферта.
12. Когато при изпълнението на договора кандидатът ще използва подизпълнител, предложението трябва да съдържа изискваните документи за идентификация и квалификация и за подизпълнителя.
13. Когато кандидат за участие в процедурата е обединение на юридически лица (консорциум) за всеки от участниците в консорциума се представят документите за идентификация и квалификация, изисквани от участниците в процедурата.
14. Всички кандидати се уведомяват за резултатите от процедурата в срок от три работни дни, считано от датата на решението на Съвета на директорите, с което се одобрява изборът на доставчик, като на избрания за изпълнител кандидат се предлага да сключи договор при условията на подаденото предложение.
15. Когато избраният за изпълнител кандидат откаже, не представи изискваните документи или по друга причина договорът с него не може да бъде подписан, изпълнителният директор предлага на класирания на следващо място кандидат да сключи договор при условията на подаденото предложение или прекратява тази и насрочва нова процедура за избор на доставчик.
16. При подписване на договора кандидатът, определен за изпълнител, представя електронно свидетелство за съдимост за удостоверяване на обстоятелствата, заявени с декларация по образец (Приложение № 5 към поканата). При невъзможност за представяне на електронно свидетелство за съдимост кандидатът представя свидетелство за съдимост или друг еквивалентен документ – сканирани и заверени с квалифициран електронен подпис. Представените документи не се съхраняват от „Информационно обслужване“ АД.