



**Български
Енергиен
Холдинг**

София 1000
ул. „Веслец“ №16
тел.: +359 2 9263 800
факс: +359 2 9250 401
<http://www.bgenh.com>

П О К А Н А

ЗА ПРЕДСТАВЯНЕ НА ЗАЯВЛЕНИЕ ЗА УЧАСТИЕ В ДОГОВАРЯНЕ С ПРЕДВАРИТЕЛЕН ПОДБОР С ПРЕДМЕТ „ДОСТАВКА И ВНЕДРЯВАНЕ НА ЦЕНТРАЛИЗИРАНО РЕШЕНИЕ ЗА РЕЗЕРВИРАНОСТ И ВЪЗСТАНОВЯВАНЕ СЛЕД БЕДСТВИЯ (DISASTER RECOVERY CENTER) ЗА НУЖДИТЕ НА ЧАСТ ОТ ДРУЖЕСТВАТА ОТ ГРУПАТА НА „БЪЛГАРСКИ ЕНЕРГИЕН ХОЛДИНГ“ ЕАД“

„Български Енергиен Холдинг“ ЕАД не е Възложител по смисъла на ЗОП.

НА ВНИМАНИЕТО НА ВСИЧКИ ЗАИНТЕРЕСОВАНИ

УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА,

С настоящото Ви каним да представите **Заявление** за участие в договаряне с предварителен подбор с предмет „Доставка и внедряване на централизирано решение за резервираност и възстановяване след бедствия (Disaster Recovery Center) за нуждите на част от дружествата от групата на „Български Енергиен Холдинг“ ЕАД“, както следва:

1.	ПРЕДМЕТ
	<p>„Доставка и внедряване на централизирано решение за резервираност и възстановяване след бедствия (Disaster Recovery Center) за нуждите на част от дружествата от групата на „Български Енергиен Холдинг“ ЕАД“.</p> <p>Целта на процедурата е да се избере изпълнител, който да достави и внедри централизирано решение за резервираност и възстановяване след бедствия (Disaster Recovery Center) за нуждите на част от дружествата от групата на „Български Енергиен Холдинг“ ЕАД (Дружеството или БЕХ ЕАД) с оглед осигуряване на непрекъсваемост на бизнес процесите в дружеството и повишаване и поддържане на високо общо ниво на мрежова и информационна сигурност съгласно чл. 12, чл. 22 и чл. 33 от Наредба за минималните изисквания за мрежова и информационна сигурност (НМИМИС).</p> <p>Обектът на поръчката е доставка.</p> <p>Подробно описание на предмета на поръчката се съдържа в Техническото задание – приложение към настоящата покана.</p>
2.	ИЗИСКВАНИЯ КЪМ КАНДИДАТИТЕ
	<p>Кандидат в настоящата процедура на договаряне с предварителен подбор може да бъде всяко българско и/или чуждестранно физическо или юридическо лице или техни обединения, както и всяко друго образувание, което отговаря на предварително обявените условия.</p>

Всеки от кандидатите в процедурата се представлява от лицето, което го представлява по закон или от упълномощено от него с нотариално заверено пълномощно лице.

2.1. Условия за участие

Всеки кандидат при подаване на заявлението си за участие представя декларация за следните обстоятелства, че :

2.1.1. Не е осъждан/а с влязла в сила присъда за престъпление по чл. 114а - 114т, чл. 159а - 159г, чл. 172, чл. 192а, чл. 194 - 217, чл. 219 - 252, чл. 253 - 260, чл. 301 - 307, чл. 321, 321а и чл. 352 - 353е от Наказателния кодекс.

2.1.2. Не е осъждан/а с влязла в сила присъда за престъпления, аналогични на тези по т. 2.1.2, в друга държава членка или трета страна;

2.1.3. Не е в производство по несъстоятелност или е обявено в несъстоятелност, или сключило извънсъдебно споразумение с кредиторите си по смисъла на чл. 740 от Търговския закон или е преустановило дейността си ;

2.1.4. Не е в производство по ликвидация и не се намира в подобна процедура съгласно националните закони и подзаконовни актове;

2.1.5. Няма парични задължения за данъци и задължителни осигурителни вноски по смисъла на чл. 162, ал. 2, т. 1 от Данъчно-осигурителния процесуален кодекс и лихвите по тях, към държавата или към общината по седалището на възложителя и на кандидата, или аналогични задължения съгласно законодателството на държавата, в която кандидатът е установен, доказани с влязъл в сила акт на компетентен орган, освен ако размерът на неплатените дължими данъци или социалноосигурителни вноски е до 1 на сто от сумата на годишния общ оборот за последната приключена финансова година, но не повече от 25 564,59 евро / 50 000,00 лв.

2.1.6. Не е установено с влязло в сила наказателно постановление или съдебно решение, нарушение на чл. 61, ал. 1, чл. 62, ал. 1 или 3, чл. 63, ал. 1 или 2, чл. 118, чл. 128, чл. 228, ал. 3, чл. 245 и чл. 301 - 305 от Кодекса на труда или чл. 13, ал. 1 от Закона за трудовата миграция и трудовата мобилност или аналогични задължения, установени с акт на компетентен орган, съгласно законодателството на държавата, в която кандидатът или кандидатът е установен.

2.1.7. Не е свързано лице с „Български Енергиен Холдинг“ ЕАД, по смисъла на § 1, т. 9 от Допълнителните разпоредби на Закона за противодействие на корупцията или със служителите на ръководна длъжност в организацията на Възложителя.

2.1.8. Не е сключил договор с лице по чл. 86 или чл. 87 от Закон за противодействие на корупцията.

(Основанията по т. 2.1.1 и 2.1.2 се отнасят за лицата, които представляват кандидата и за членовете на неговите управителни и надзорни органи съгласно регистъра, в който е вписан кандидатът, ако има такъв, или документите, удостоверяващи правосубектността му. Когато в състава на тези органи участва юридическо лице, основанията се отнасят за физическите лица, които го представляват съгласно регистъра, в който е вписано юридическото лице, ако има такъв, или документите, удостоверяващи правосубектността му

В посочените случаи, когато кандидатът или участникът, или юридическо лице в състава на негов контролен или управителен орган се представлява от физическо лице по пълномощие, основанията по т. 1 и 2 се отнасят и за това физическо лице.

По отношение на обстоятелства по т. 2.1.1 и 2.1.2, основанията се прилагат пет години от влизането в сила на присъдата, освен ако в присъдата е посочен друг срок на наказанието.

Обстоятелствата по т. 2.1.4 и по т. 2.1.5 се декларират от членовете на управителните и контролните органи на ЮЛ, включително и от временно изпълняващите тази длъжност и от прокуристите и търговските пълномощници.

** „Свързани лица“ са съпрузите или лицата, които се намират във фактическо съжителство, роднините по права линия, по сребрена линия - до четвърта степен включително, и роднините по сватовство - до втора степен включително, както и*

физически и юридически лица, с които лицето, заемащо публична длъжност, се намира в икономически или политически зависимости, които пораждат основателни съмнения в неговата безпристрастност и обективност.)

Доказване на изискванията по 2.1.: Кандидатът удостоверява обстоятелствата по точки от 2.1.1. до 2.1.8. с Декларация по образец (Приложение №3).

2.2. Изисквания и доказателства за икономическо и финансово състояние:

Кандидатът да е реализирал минимален оборот в сферата, попадаща в обхвата на поръчката за последните три финансови години, в зависимост от датата, на която е учреден или е започнал дейността си.

Минимално изискване:

Кандидатът да е реализирал минимален оборот в сферата, попадаща в обхвата на поръчката за последните три финансови години, в зависимост от датата, на която е учреден или е започнал дейността си в размер на 2,500,000.00 (два милиона и петстотин хиляди) евро/ 4 889 575 (четири милиона осемстотин осемдесет и девет хиляди петстотин седемдесет и пет) лева.

Под „оборот в сферата, попадаща в обхвата на поръчката“ следва да се разбира доставка, инсталация/внедряване на информационни и комуникационни системи.

Обстоятелството се доказва чрез:

- Декларация за оборота в сферата, попадаща в обхвата на поръчката, за последните три приключили финансови години (Приложение №5).
- Заверено от кандидата копие на ОПР и баланс за последните 3 (три) приключили финансови години (2023, 2024 и 2025), в зависимост от датата, на която кандидатът е учреден или е започнал дейността си. Кандидатите могат да посочат ЕИК и да не представят изискваните документи по предходното изречение, в случай че са заявили и представили за обявяване годишния финансов отчет за съответните години в Търговския регистър и регистър на ЮЛНЦ, съгласно чл. 38 от Закона за счетоводството и същите са публично достъпни.

Кандидатите – чуждестранни лица, представят заверени копия от баланса и отчета за приходите и разходите като съставна част от годишния финансов отчет, когато публикуването им се изисква от законодателството на държавата, в която са установени.

2.3. Изисквания и доказателства за технически възможности:

2.3.1. Кандидатът трябва да е изпълнил дейности с предмет и обем, идентични или сходни с този на настоящата поръчка за последните 3 (три) години от датата на подаване на заявлението.

Минимално изискване:

За последните 3 (три) години, считано до крайната дата за подаване на заявление, кандидатът трябва да има изпълнен минимум 1 (един) договор с предмет, сходен с предмета на поръчката.

Забележка: Под сходен предмет следва да се разбира доставка, инсталация/внедряване на информационни и комуникационни системи.

Под „изпълнен“ договор следва да се разбира такъв, който независимо от датата на сключването му е приключил в посочения по-горе период.

Обстоятелството се доказва чрез:

- Списък на изпълнени договори с идентичен или сходен предмет, съгласно приложен образец (Приложение №6);
- Посочен линк към публичен регистър и/или приложени референции и/или други документи, от които да е видно, че договорите са изпълнени качествено и в срок.

	<p>2.3.2. Кандидатът трябва да има внедрена система за управление на качеството ISO 9001:2015 или еквивалент с обхват на сертификацията, включващ доставка, инсталация и внедряване на информационни и комуникационни системи, издаден от независими лица, акредитирани по съответната серия европейски стандарти от Изпълнителна агенция „Българска служба за акредитация” или от друг национален орган за акредитация, който е страна по Многостранното споразумение за взаимно признаване на Европейската организация за акредитация за съответната област или да отговаря на изискванията за признаване съгласно чл. 5а, ал. 2 от Закона за националната акредитация на органи за оценяване на съответствието.</p> <p><u>Обстоятелството се доказва чрез:</u></p> <ul style="list-style-type: none"> - <i>Заверено копие „вярно с оригинала“ на валиден сертификат БДС EN ISO 9001:2015 за внедрена система за управление на качеството или еквивалентен.</i> <p>2.3.3. Кандидатът трябва да има внедрена система за управление на сигурността на информацията ISO 27001:2013 или еквивалент с обхват на сертификацията, включващ доставка, инсталация и внедряване на информационни и комуникационни системи, издаден от независими лица, акредитирани по съответната серия европейски стандарти от Изпълнителна агенция „Българска служба за акредитация” или от друг национален орган за акредитация, който е страна по Многостранното споразумение за взаимно признаване на Европейската организация за акредитация за съответната област или да отговаря на изискванията за признаване съгласно чл. 5а, ал. 2 от Закона за националната акредитация на органи за оценяване на съответствието.</p> <p><u>Обстоятелството се доказва чрез:</u></p> <ul style="list-style-type: none"> - <i>Заверено копие „вярно с оригинала“ на валиден сертификат БДС EN ISO 27001:2013 за внедрена система за управление на сигурността на информацията или еквивалентен.</i> <p>2.3.4. Кандидатът трябва да има внедрена система за управление на услугите ISO 200001-1:2018 или еквивалент с обхват на сертификацията, включващ поддръжка на решения в областта на информационните и комуникационните технологии, издаден от независими лица, акредитирани по съответната серия европейски стандарти от Изпълнителна агенция „Българска служба за акредитация” или от друг национален орган за акредитация, който е страна по Многостранното споразумение за взаимно признаване на Европейската организация за акредитация за съответната област или да отговаря на изискванията за признаване съгласно чл. 5а, ал. 2 от Закона за националната акредитация на органи за оценяване на съответствието.</p> <p><u>Обстоятелството се доказва чрез:</u></p> <ul style="list-style-type: none"> - <i>Заверено копие „вярно с оригинала“ на валиден сертификат БДС EN ISO 200001-1:2018 за внедрена система за управление услугите или еквивалентен.</i> <p>Кандидатът, в случай, че не е производител на предлаганото хардуерно оборудване и софтуер, следва да представи актуално оторизационно писмо или друг документ, издаден от производителя/ите, с правомощия за територията на Република България, или от самите производители на марките, с които кандидатът участва, в уверение че е оторизиран да предлага техниката и софтуера, предмет на офертата. Оторизационният документ трябва да бъде издаден на името на кандидата.</p>
3.	КОМУНИКАЦИЯ МЕЖДУ ВЪЗЛОЖИТЕЛЯ И КАНДИДАТИТЕ

	<p>3.1 Всички комуникации между Възложителя и кандидатите, свързани с настоящата процедура, се осъществяват в писмен вид.</p> <p>3.2 Обменът на информация между Възложителя и кандидата може да се извършва по един от следните начини:</p> <ul style="list-style-type: none"> - лично – срещу подпис; - по пощата – чрез препоръчано писмо с обратна разписка; - чрез куриерска служба; - чрез електронна поща. <p>3.3 Възложителят има право да прави промени в Поканата и приложенията към нея, свързани с отстраняване на пропуски, явна фактическа грешка или удължаване на срока за подаване на заявления.</p> <p>3.4 Всеки кандидат може да поиска писмено разяснения по Поканата до 12:00 ч. на 23.03.2026г.</p> <p>3.5 Всички разяснения ще бъдат публикувани на интернет страницата на „Български Енергиен Холдинг“ ЕАД до 17:30 ч. на 23.03.2026г.</p>
4.	ПРЕДСТАВЯНЕ НА ЗАЯВЛЕНИЯ
	<p>4.1. За участие в договаряне с предварителен подбор, кандидатът подготвя и представя заявление, което трябва да съответства напълно на изискванията и указанията в настоящата Покана.</p> <p>4.2. Срокът за представяне на заявленията е до 16:00 ч. на 24.03.2026г.</p> <p>4.3. Всеки кандидат има право да представи само едно заявление.</p> <p>4.4. Заявлението се подава на български език. Документи, съставени на езици различни от български език, се представят, придружени с официален превод на български език.</p> <p>4.5. Заявлението следва да бъде представено на адреса, посочен в настоящата Покана, преди посочения краен срок за представяне на заявленията.</p> <p>4.6. Заявлението се представя в запечатан непрозрачен плик от кандидата или от упълномощен от него представител, лично или по пощата с препоръчано писмо с обратна разписка, или чрез куриерска служба на адрес: гр. София 1000, ул. „Веслец“ №16. Върху плика кандидатът посочва следните означения: „ЗАЯВЛЕНИЕ“, име на кандидата, предмет на процедурата, адрес и лице за кореспонденция, телефон и електронен адрес.</p> <p>4.7. Получените заявления се завеждат в деловодния регистър на „Български Енергиен Холдинг“ ЕАД, като всяко получава регистрационен номер с дата и час.</p> <p>4.8. В случай, че кандидат изпраща заявлението си чрез препоръчана поща или куриерска служба, разходите са за сметка на кандидата. В този случай, той следва да изпрати заявлението така, че да обезпечи пристигането му на посочения от Възложителя адрес преди изтичане на срока за подаване на заявления. Рискът от забава или загубване на заявлението е за кандидата.</p> <p>4.9. Всички разходи на кандидата за участие в процедурата са за негова сметка.</p>
5.	ПРОВЕЖДАНЕ НА ДОГОВАРЯНЕ С ПРЕДВАРИТЕЛЕН ПОДБОР
	<p>5.1. За провеждане на договаряне с предварителен подбор Възложителят назначава комисия с писмена заповед. При необходимост комисията може по всяко време да проверява заявените от кандидатите данни, включително чрез изискване на информация от други органи и лица, да изисква от кандидатите разяснения на заявени от тях данни, както и допълнителни доказателства за данни от документите. Комисията разглежда заявленията по реда на тяхното постъпване и извършва подбор на лицата въз основа на представените документи.</p> <p>5.2. Кандидати, които не отговарят на изискванията и условията, посочени в настоящата покана, няма да бъдат поканени да подадат оферти.</p> <p>5.3. Резултатите от подбора се отразяват в протокол, който се утвърждава от Възложителя.</p>

	<p>5.4. Възложителят изпраща покана за подаване на оферти до лицата, определени въз основа на предварителния подбор.</p> <p>5.5. Комисията разглежда постъпилите оферти за съответствие с изискванията на Възложителя и съставя протокол/и, след което провежда преговори с участниците за постигане на по-благоприятни условия за Възложителя и за определяне клаузите на договора.</p> <p>5.6. Възложителят запазва правото си, по свое усмотрение, да прекрати процедурата и да не подпише договор, без това да води до каквито и да било правни и/или финансови последици за него. В горепосочените случаи, Възложителят не може да бъде подведен под отговорност за претърпени вреди или пропуснати ползи.</p> <p>5.7. Възложителят уведомява писмено кандидатите или участниците в случай на прекратяване на процедурата.</p>
6.	СЪДЪРЖАНИЕ НА ЗАЯВЛЕНИЕТО
	<p>Всички представени копия на документи следва да бъдат заверени „Вярно с оригинала“.</p> <p><i>Заявлението следва да съдържа:</i></p> <p>6.1 Списък на представените документи, съдържащи се в заявлението за участие (препоръчително е описанието в списъка да съответства на настоящата подредба и на подредбата на документите в заявлението). <i>(Приложение №1)</i></p> <p>6.2 Административни сведения за кандидата, съгласно приложен образец <i>(Приложение №2)</i>.</p> <p>6.3 Пълномощно на лицето, подписващо заявлението (оригинал) – представя се, когато заявлението (както и други документи) не са подписани от представляващия/те кандидата съгласно актуалното му състояние, а от изрично упълномощен негов представител – когато е приложимо.</p> <p>6.4 Декларация за отсъствие на обстоятелства по т. 2.1.1 до 2.1.6. съгласно приложен образец <i>(Приложение №3)</i>.</p> <p>6.5 Декларация за конфиденциалност съгласно приложен образец <i>(Приложение №4)</i>.</p> <p>6.6 Декларация за оборота в сферата, попадаща в обхвата на поръчката, за последните три години, съгласно приложен образец <i>(Приложение №5)</i>.</p> <p>6.7 Заверено от кандидата копие на ОПР и баланс за последните 3 (три) приключили финансови години (2023, 2024 и 2025), в зависимост от датата, на която кандидатът е учреден или е започнал дейността си.</p> <p>6.8 Списък на изпълнените договори съгласно приложен образец <i>(Приложение №6)</i>.</p> <p>6.9 Доказателства за добро изпълнение за минимум 1 (един) от включените в списъка договори, например, посочване на публични регистри, в които е налична информация за доброто изпълнение и/или приложени референции/препоръки за добро изпълнение.</p> <p>6.10 Заверено копие „вярно с оригинала“ на валиден сертификат ISO 9001:2015 или еквивалент.</p> <p>6.11 Заверено копие „вярно с оригинала“ на валиден сертификат ISO 27001:2013 или еквивалент.</p> <p>6.12 Заверено копие „вярно с оригинала“ на валиден сертификат ISO 200001-1:2018 или еквивалент.</p> <p>6.13 Заверено копие „вярно с оригинала“ на оторизационно писмо, издадено от производителя на предложеното хардуерно оборудване и софтуер.</p> <p>6.14 Техническо задание <i>(Приложение №7)</i>.</p>
	<u>Забележки:</u>
	<p>1. Възложителят има право да изисква разяснения по представените документи и информация.</p>

	<p>2. Възложителят запазва правото си да отстрани от по-нататъшно участие в договарянето кандидат, чието заявление не отговаря на горепосочените изисквания.</p> <p>3. Представените образци в документацията за участие и условията, описани в тях, са задължителни за кандидатите и не могат да бъдат променяни от тях.</p>
7.	ЗА ИНФОРМАЦИЯ:
	Електронна поща: dr@bgenh.com

Очакваме Вашите заявления.

Неразделна част от настоящата Покана са следните приложения:

Приложение №	1	Списък на представените документи
Приложение №	2	Административни сведения за кандидата;
Приложение №	3	Декларация за отсъствие на обстоятелства;
Приложение №	4	Декларация за конфиденциалност;
Приложение №	5	Декларация за оборота в сферата, попадаща в обхвата на поръчката, за последните три години;
Приложение №	6	Списък на изпълнени договори с идентичен или сходен предмет;
Приложение №	7	Техническо задание;

Списък с представените документи, съдържащи се в заявлението за участие в договаряне с предварителен подбор с предмет: „Доставка и внедряване на централизирано решение за резервираност и възстановяване след бедствия (Disaster Recovery Center) за нуждите на част от дружествата от групата на „Български Енергиен Холдинг“ ЕАД“

Кандидат:, с БУЛСТАТ/ЕИК/Номер на регистрация в съответната държава
[.....]

№	Съдържание	Вид и количество на документите <i>/оригинал или заверено копие и общ брой страници/</i>
1.	Административни сведения на кандидата (по образец)	
2.	Удостоверение за актуално състояние, справка от Търговския регистър и регистъра на ЮЛНЦ, копие от документа за регистрация или единен идентификационен код съгласно чл. 23 от Закона за търговския регистър и регистъра на ЮЛНЦ <i>(Посочват се и се описват документа/ите, който/които са представени)</i>	
3.	Пълномощно на лицето, подписващо заявлението/офертата <i>(когато не е подписана от представляващия и управляващия кандидата)</i>	
4.	Декларация за отсъствие на обстоятелствата по т. 2.1.1. до 2.1.6. от поканата (по образец)	
5.	Декларация за конфиденциалност (по образец)	
6.	Доказателства за икономическо и финансово състояние, както и за техническите възможности на кандидата (съгласно т. 2.2. и т. 2.3. от поканата и приложените към поканата образци), както следва: <i>(Посочват се и се описват документа/ите, който/които са представени)</i>	
7.	Списък на изпълнените договори с идентичен и/или сходен предмет	
8.	Доказателства за добро изпълнение на включените в списъка договори	

[дата]

ПОДПИС

ПЕЧАТ

[име и фамилия]

[качество на представляващия кандидата]

АДМИНИСТРАТИВНИ СВЕДЕНИЯ

за участие в договаряне с предварителен подбор с предмет „Доставка и внедряване на централизирано решение за резервираност и възстановяване след бедствия (Disaster Recovery Center) за нуждите на част от дружествата от групата на „Български Енергиен Холдинг“ ЕАД“

.....

1. ИДЕНТИФИКАЦИЯ НА КАНДИДАТА

Настоящото заявление е подадено от

	<i>наименование на кандидата</i>
регистр. с Решение от ... / на
по ф. дело № .../ ... г.,
с адрес на управление:
ЕИК
Ид № по ДДС
банкова сметка IBAN
банков код
обслужваща банка
и подписана от:
	<i>трите имена и ЕГН</i>
в качеството му на:
	<i>длъжност</i>

2. АДМИНИСТРАТИВНИ СВЕДЕНИЯ ЗА КАНДИДАТА

1. Адрес
	<i>код, град, община, квартал, улица, бл., ап.</i>
2. Телефон
3. Факс
4. e-mail
5. интернет адрес
6. Лице за контакт
/име, длъжност/

[дата]

ПОДПИС

ПЕЧАТ

[име и фамилия]

[качество на представляващия кандидата]

ДЕКЛАРАЦИЯ
за липса на обстоятелства

Долуподписаният/ната _____ с ЕГН _____, в качеството ми на _____ (посочва се заеманата длъжност) на _____ (посочва се фирмата на кандидата), с БУЛСТАТ/ ЕИК _____, със седалище и адрес на управление: _____,

кандидат в договаряне с предварителен подбор с предмет: „Доставка и внедряване на централизирано решение за резервираност и възстановяване след бедствия (Disaster Recovery Center) за нуждите на част от дружествата от групата на „Български Енергиен Холдинг“ ЕАД“

ДЕКЛАРИРАМ¹, ЧЕ:

1. Не съм осъден/а с влязла в сила присъда за престъпление по чл. 114а - 114т, чл. 159а - 159г, чл. 172, чл. 192а, чл. 194 - 217, чл. 219 - 252, чл. 253 - 260, чл. 301 - 307, чл. 321, 321а и чл. 352 - 353е от Наказателния кодекс.

2. Не съм осъден/а с влязла в сила присъда за престъпления, аналогични на тези по т. 1, в друга държава членка или трета страна.

3. Представляваното от мен дружество:

а) не е в производство по несъстоятелност или е обявено в несъстоятелност, или сключило извънсъдебно споразумение с кредиторите си по смисъла на чл. 740 от Търговския закон или е преустановило дейността си ;

б) не е в производство по ликвидация и не се намира в подобна процедура съгласно националните закони и подзаконови актове;

в) няма парични задължения за данъци и задължителни осигурителни вноски по смисъла на чл. 162, ал. 2, т. 1 от Данъчно-осигурителния процесуален кодекс и лихвите по тях, към държавата или към общината по седалището на възложителя и на кандидата, или аналогични задължения съгласно законодателството на държавата, в която кандидатът е установен, доказани с влязъл в сила акт на компетентен орган, освен ако размерът на неплатените дължими данъци или социалноосигурителни вноски е до 1 на сто от сумата на годишния общ оборот за последната приключена финансова година, но не повече от 25 564,59 евро / 50 000,00 лв.

г) не е установено с влязло в сила наказателно постановление или съдебно решение, нарушение на чл. 61, ал. 1, чл. 62, ал. 1 или 3, чл. 63, ал. 1 или 2, чл. 118, чл. 128, чл. 228, ал. 3, чл. 245 и чл.

¹ Основанията по т. 1 и 2 се отнасят за лицата, които представляват кандидата и за членовете на неговите управителни и надзорни органи съгласно регистъра, в който е вписан кандидатът, ако има такъв, или документите, удостоверяващи правосубектността му. Когато в състава на тези органи участва юридическо лице, основанията се отнасят за физическите лица, които го представляват съгласно регистъра, в който е вписано юридическото лице, ако има такъв, или документите, удостоверяващи правосубектността му.

В посочените случаи, когато кандидатът или участникът, или юридическо лице в състава на негов контролен или управителен орган се представлява от физическо лице по пълномощие, основанията по т. 1 и 2 се отнасят и за това физическо лице.

По отношение на обстоятелства по т. 1 и 2, основанията се прилагат пет години от влизането в сила на присъдата, освен ако в присъдата е посочен друг срок на наказанието.

Обстоятелствата по т.4 и по т.5 се декларират от членовете на управителните и контролните органи на ЮЛ, включително и от временно изпълняващите тази длъжност и от прокуристите и търговските пълномощници.

301 - 305 от Кодекса на труда или чл. 13, ал. 1 от Закона за трудовата миграция и трудовата мобилност или аналогични задължения, установени с акт на компетентен орган, съгласно законодателството на държавата, в която кандидатът или участникът е установен.

4. Не съм свързано лице² по смисъла на § 1, т. 9 от Допълнителната разпоредба на Закона за противодействие на корупцията с „Български Енергиен Холдинг“ ЕАД и/или с член/членовете на Съвета на директорите на БЕХ ЕАД.

5. За мен лично и представляваното от мен юридическо лице не са налице обстоятелствата по чл. 86 или 87 от Закона за противодействие на корупцията.

Известно ми е, че за деклариране на неверни данни нося отговорност по чл. 313 от НК.

[дата]

ПОДПИС

ПЕЧАТ

[име и фамилия]

[качество на представляващия кандидата]

² „Свързани лица“ са съпрузите или лицата, които се намират във фактическо съжителство, роднините по права линия, по сребрена линия - до четвърта степен включително, и роднините по сватовство - до втора степен включително, както и физически и юридически лица, с които лицето, заемащо публична длъжност, се намира в икономически или политически зависимости, които пораждат основателни съмнения в неговата безпристрастност и обективност.

ДЕКЛАРАЦИЯ
за конфиденциалност

Долуподписаният/ната _____ с ЕГН _____, в качеството ми на _____ (посочва се заеманата длъжност) на _____ (посочва се фирмата на кандидата), с БУЛСТАТ/ ЕИК _____, със седалище и адрес на управление: _____,

кандидат в договаряне с предварителен подбор с предмет: „Доставка и внедряване на централизирано решение за резервираност и възстановяване след бедствия (Disaster Recovery Center) за нуждите на част от дружествата от групата на „Български Енергиен Холдинг“ ЕАД“

ДЕКЛАРИРАМ, ЧЕ:

1. Няма да използвам и оповестявам пред трети лица сведения и факти, станали ми известни при участие в договаряне с предварителен подбор с предмет: „Доставка и внедряване на централизирано решение за резервираност и възстановяване след бедствия (Disaster Recovery Center) за нуждите на част от дружествата от групата на „Български Енергиен Холдинг“ ЕАД“

2. Няма да злоупотребявам с доверието и да уронвам името на „Български Енергиен Холдинг“ ЕАД.

[дата]

ПОДПИС

ПЕЧАТ

[име и фамилия]

[качество на представляващия кандидата]

Наименование: [наименование на кандидата],
Регистрация: [данни за регистрацията]
Представяван от [трите имена на представляващия] в качеството на [длъжност, или друго качество]
с БУЛСТАТ/ЕИК [...], регистрирано в [...], със седалище [...] и адрес на управление [...],

ДЕКЛАРАЦИЯ

за оборот от дейности, идентични и/или сходни с предмета на процедурата, за последните три години

Долуподписаният/ната _____ с ЕГН _____, в качеството ми на _____ (посочва се заеманата длъжност) на _____ (посочва се фирмата на кандидата), с БУЛСТАТ/ ЕИК _____, със седалище и адрес на управление: _____, кандидат в договаряне с предварителен подбор с предмет: „Доставка и внедряване на централизирано решение за резервираност и възстановяване след бедствия (Disaster Recovery Center) за нуждите на част от дружествата от групата на „Български Енергиен Холдинг“ ЕАД“

ДЕКЛАРИРАМ следното:

	2023 г.	2024 г.	2025 г.	Общо
Оборот от дейности в сферата, попадаща в обхвата на поръчката				

Известно ми е, че за вписване на неверни данни в настоящата декларация подлежа на наказателна отговорност съгласно чл. 313 от Наказателния кодекс.

[дата]

ПОДПИС

ПЕЧАТ

[име и фамилия]

[качество на представляващия кандидата]

Наименование: [наименование на кандидата],

Регистрация: [данни за регистрацията]

Представяван от [трите имена на представляващия] в качеството на [длъжност, или друго качество]

с БУЛСТАТ/ЕИК [...], регистрирано в [...], със седалище [...] и адрес на управление [...],

СПИСЪК

на изпълнени договори с идентичен и/или сходен предмет за участие в договаряне с предварителен подбор с предмет: „Доставка и внедряване на централизирано решение за резервираност и възстановяване след бедствия (Disaster Recovery Center) за нуждите на част от дружествата от групата на „Български Енергиен Холдинг“ ЕАД“

№	Обект (предмет) на договора	Възложител /Получател [име; лице за контакт; адрес; телефон; e-mail]	Стойност на договора	Начална – крайна дата на договора	В качеството на: [главен изпълнител; участник в обединение; подизпълнител]
1	2	3	4	5	6

В подкрепа на посочените в списъка договори изпълнени от нас, прилагаме следните доказателства:

Изброяват се приложените от кандидата документи (Напр.: препоръки/референции за добро изпълнение) или конкретните публични регистри, в които е налична информация и на които той се позовава. Кандидатът може да прилага или да се позовава на едно или повече от изброените.

[дата]

ПОДПИС

ПЕЧАТ

[име и фамилия]

[качество на представляващия кандидата]

ТЕХНИЧЕСКО ЗАДАНИЕ

Възложителят провежда настоящата процедура с цел избор на изпълнител за „Доставка и внедряване на централизирано решение за резервираност и възстановяване след бедствия (Disaster Recovery Center) за нуждите на част от дружествата от групата на „Български Енергиен Холдинг“ ЕАД“, при следните условия:

I. Цел на процедурата:

Центърът за резервираност (Disaster Recovery Center) следва да обслужва стратегически важните информационни системи на следните енергийните дружества от групата на БЕХ ЕАД – „АЕЦ Козлодуй“ ЕАД, „ТЕЦ Марица изток 2“ ЕАД, „Национална електрическа компания“ ЕАД, „Булгаргаз“ ЕАД и „Мини Марица-изток“ ЕАД, като целите са:

1. Подсигуряване работата на критични информационни системи на дружествата от групата на „Български Енергиен Холдинг“ ЕАД при частично или цялостно отпадане на основния център за данни;
2. Осигуряване на висока надеждност, наличност, резервираност и устойчивост на информационните системи и гарантиране на ефективната работа;
3. Намаляване до минимум на вероятността от загуба на работоспособност на системите, загуба на данни, частично или пълно отпадане на услуги и системи при непредвидени инциденти с основните ресурси на продукционната среда;
4. Изпълнение на нормативните изисквания на чл. 32 и чл. 33 от „Наредбата за минималните изисквания за мрежова и информационна сигурност“ по отношение на осигуряването на устойчивост, резервиране и архивиране на информация и резервиране на компоненти на инфраструктурата на дружества от групата на Български Енергиен Холдинг ЕАД.

II. ОБЩИ ИЗИСКВАНИЯ ЗА ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА

1. Участникът трябва да предложи цялостно решение, включващо хардуер и софтуер, както и всички прилежащи услуги към тях за въвеждането им в експлоатация.
2. Предлаганото оборудване трябва да отговоря на следните изисквания:
 - Да бъде ново, оригинално, неупотребявано, в производствената листа на производителя за текущата година;
 - Да бъде в пълно работно състояние, в оригиналната опаковка на производителя с не нарушена цялост, придружено със съответните документи за произход и качество;
 - Да бъде окомплектовано с всички необходими интерфейси, хранящи кабели и крепежни елементи;
3. Доставеното оборудване трябва да се монтира в 2 броя сървърни шкафове на Възложителя, намиращи се в локация на адрес в гр. София.
4. Предлаганата от кандидатите гаранционна (техническа) поддръжка от производителя трябва да бъде със срок на валидност **минимум 36 (тридесет и шест) месеца**, считано от датата на въвеждане в експлоатация и подписване на приемо-предавателен протокол и да включва:
 - Ниво на обслужване: 24x7x365 достъп до Център за техническа помощ, с възможност за докладване на проблеми, възникнали при работа.
 - Времето за реакция да е до 2 часа след уведомяването за възникнал проблем, чрез регистриране на сервизна заявка в Център за техническа помощ. Възстановяване на работоспособност на дефектирало оборудване се извършва на следващия ден. Ако повредата не може да бъде отстранена в рамките на определения срок, дефектиралото устройство следва да бъде заменено най-късно до следващия работен ден със същото или еквивалентно - отговарящо на минималните технически изисквания от Техническата спецификация.

- Възможност за получаване на нови версии на софтуерните системи – **минимум 36 (тридесет и шест) месеца**, считано от датата на доставка и подписване на приемо-предавателен протокол.

5. Услуги по възстановяване на системи и инфраструктура, които следва да бъдат осигурени от изпълнителя за срока на договора (DR услуги).

- Изпълнителят осигурява екип от специалисти, които да поддържат системите за архивиране и възстановяване актуални и налични 24/7/365 (в т.ч. репликации, backup процеси, инфраструктура);
- Времето за реакция при необходимост от задействане на процедура по възстановяване да бъде в рамките на 30 мин. след подаване на заявка в център за техническа помощ на изпълнителя.
- Процедурите по възстановяване на информационни ресурси да бъдат съобразени с действащите DR планове на дружествата, които ще бъдат обслужвани (синхронизирне на RTO и RPO, failover/fallback процедури, dependency mapping между системите и ред за стартиране при възникнала необходимост);
- Репликация и защита на данни (осигуряване на репликация между основен и DR сайт, бекъп политики, съхранение и защита от ransomware, чрез “immutable backup/storage systems”)
- Тестване и валидиране (периодични restore тестове при различни сценарии, като срыв, ransomware, отпадане на основен data център и проверка на бекъпи)
- Предоставяните услуги по възстановяване на системи и инфраструктура да отговарят на международни стандарти за управление на непрекъсваемостта на бизнеса ISO 22301, за управление на сигурността на информацията от серията ISO 27001, както и frameworks дефиниращи качеството на услугата.

6. Общият срок за изпълнение на поръчката – до **180 дни**, считано от датата на подписване на договора.

II. ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ:

1. Софтуерна платформа за архивиране, възстановяване и репликация на данни - 1 брой, със следните минимални технически параметри и функционалности:

Параметър	Технически изисквания на възложителя
марка, модел и продуктов номер	Посочва се от участника
Тип на лиценза	Абонаментен за предложения период на поддръжка
Брой лицензи	20 броя
Архивиране и възстановяване	- Възстановяване на ниво файл, обект и виртуална машина - Архивиране от сторидж снапшоти - Вградена WAN оптимизация
Репликация и възстановяване	Периодична репликация на виртуални машини
Мониторинг и анализи	- Централизиран мониторинг на бекъп задачи и ресурси - Капацитетно планиране
Автоматизация на аварийното възстановяване	- Тестове на DR планове - Автоматично документиране на DR процесите

Сигурност и съответствие	RBAC (управление на роли и достъп)
Съвместимост със следните виртуални среди и операционни системи	- VMware vSphere 6.5 или по-нова, Microsoft Hyper-V Server 2016 или по-нова - Windows Server 2012 R2 или по-нова

2. Софтуерна платформа за виртуализация, управление, съхранение, мрежова сигурност и автоматизация - 1 брой, със следните минимални технически параметри и функционалности:

Параметър	Технически изисквания на възложителя
марка, модел, продуктов номер и линк към сайта на производителя	Посочва се от участника
Тип на лиценза	Абонаментен за предложения период на поддръжка
Брой лицензи	За 1152 броя физически ядра
Обща функционалност	Предложената софтуерна платформа за инфраструктура да бъде като услуга (IaaS), която да предоставя софтуерно дефинирани изчисления, съхранение, мрежи, сигурност и управление.
Надеждност и скалируемост	Да има вградено автоматично мащабиране и клъстериране за непрекъсната работа.
Автоматизация	- Да поддържа интегрирана автоматизация за бързо разполагане на виртуални машини. - Да осигурява автоматизация и оркестрация за задачи от тип Day 0, Day 1 и Day 2. - Да осигурява автоматизирано управление на жизнения цикъл, провизиране на приложения/инфраструктура
Висока наличност	Да гарантира непрекъсната работа на всяко приложение при хардуерен отказ, без загуба на данни или време за възстановяване.
Сигурност	Да шифрира данните на виртуалните машини (data-at-rest) и свързаните с тях дискове.
Съхранение	- Да позволява съхраняване на данни, използваща RAID 5 или RAID 6 с производителност, съпоставима с RAID 1. - Да осигурява контролен панел за управление както на облачно, така и на файлово съхранение. - Да провизира файл-системи чрез единен работен процес (workflow).
Оперативни възможности	Да разполага с интегрирани инструменти за: - Оптимизация на производителността - Управление на капацитета - Мониторинг и отстраняване на проблеми

	<ul style="list-style-type: none"> - Анализ на логове - Вграден мониторинг на приложения чрез Telegraf агент
Софтуерно-дефинирани мрежи (SDN)	- Да поддържа пълноценно моделиране и създаване на мрежови топологии – от прости до многослойни.
Мрежови функции	<p>Да предоставя логически мрежови услуги, включително:</p> <ul style="list-style-type: none"> - Логическо превключване (Logical Switching) - Маршрутизиране (Routing) - Разпределено балансиране на натоварването (Distributed Load Balancing) - Виртуална частна мрежа (VPN) - Управление на качеството на услугата (QoS) - Мониторинг
Виртуален частен облак (VPC)	Да осигурява изолирани мрежови среди в рамките на споделена инфраструктура.
Тип на поддръжката	24x7, с достъп до актуализации и пачове (корекции) по време на абонаментния период.

3. Софтуерна платформа за възстановяване на виртуални машини - 1 брой, със следните минимални технически параметри и функционалности:

Параметър	Технически изисквания на възложителя
марка, модел, продуктов номер и линк към сайта на производителя	<ul style="list-style-type: none"> - Посочва се от участника - Да бъде от производителя на предложената платформа за виртуализация
Тип на лиценза	Абонаментен за предложения период на поддръжка
Брой лицензи	За 700 броя виртуални машини
Типове възстановяване в случай на срив или отказ в инфраструктурата	- Да поддържа мин. два вида възстановяване от защитения сайт
Интеграция с репликация	Да използва механизми за репликация за минимизиране на загуба на данни и време на неработоспособност.
Управление на виртуални машини (VM)	<ul style="list-style-type: none"> - при активен защитен сайт да изключва VM коректно и да синхронизира съхранението. - да включва репликираните VM на сайта за възстановяване съгласно план за възстановяване.
Възстановителен план	<ul style="list-style-type: none"> - да определя реда на стартиране на VM. - да конфигурира мрежови параметри (напр. IP адреси). - да позволява добавяне на потребителски скриптове за персонализирани действия.

Тестване на възстановяването	Да позволява тестване чрез временни копия на репликирани данни, без прекъсване на продукционната работа в двата сайта.
Тип на поддръжката	24x7, с достъп до актуализации и пачове (корекции) по време на абонаментния период.

4. Софтуерна платформа за управление на защитни стени - 1 брой, със следните минимални технически и функционални параметри:

Параметър	Технически изисквания на възложителя
марка, модел, продуктов номер и линк към сайта на производителя	Посочва се от участника
Съвместимост	Да е съвместима с предложените от участника защитни стени
Съвместимост	Да позволява инсталация върху виртуална машина, работеща във VMware и HyperV среда за виртуализация;
Управление	Да позволява управлението на минимум 25 защитни стени (устройства, виртуални защитни стени или виртуални контекста)
Управление	Да позволява налагането на политики за сигурност чрез предварително дефинирани профили (Templates)
Управление	Да позволява централизирана конфигурация на защитните стени като: интерфейси маршрутизиращи протоколи
Управление	Да позволява групиране на устройствата и създаване на йерархична структура
Управление	Да позволява централизирано внедряване на актуализации и нови версии
Мониторинг	Да позволява събиране, съхранение и анализ на логове
Мониторинг	Да разполага с предварително дефинирани отчети, които да могат да се генерират отделно или по групи
Мониторинг	Да разполага с доклади за активност на потребителите използваните приложения, посетени URL категории, уебсайтове посетени URL адреси, за определен период от време за отделни потребители.
Автоматизация	Да позволява автоматизирано внедряване на политики за динамични среди
Автоматизация	Да предлага базирани на XML и JSON REST API за лесна интеграция
Тип на поддръжката	24x7, с достъп до актуализации и пачове (корекции) по време на абонаментния период.

5. Защитни стени - 2 броя, със следните минимални технически и функционални параметри:

Параметър	Технически изисквания на възложителя
марка, модел, продуктов номер и линк към сайта на производителя	Посочва се от участника
Общо изискване	<ul style="list-style-type: none"> - Предложените 2 устройства да са 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 минималните технически параметри по-долу
Пропускателна способност с активирана функция за идентификация на приложенията	90.0 Gbps
Пропускателна способност с активирани всички функционалности за защита: IPS/ AntiVirus/ Anti-Malware / URL / Firewall / Application Control	75 Gbps
Производителност за IPsec VPN	60 Gbps
Брой TCP сесии	45 000 000
Брой нови сесии в секунда	440 000
Разпознати и поддържани приложения	5 100
Брой мрежови интерфейси	<ul style="list-style-type: none"> - 8x 1G/2.5G/5G/10G Base-T - 2x 10G SFP+ ports - Допълнителни слотове за надграждане минимум: <ul style="list-style-type: none"> - 10x 10G SFP+ - 4x 40G/100G QSFP+/QSFP28 - 4x 25G SFP28
Режими на работа на интерфейсите	L2, L3, Tap, Transparent едновременно/микс да се използват върху едно устройство.
Машрутизащи протоколи	- OSPFv2/v3, BGP with graceful restart, RIP, static routing Policy-based forwarding

	<ul style="list-style-type: none"> - Point-to-Point Protocol over Ethernet (PPPoE) - Bidirectional Forwarding Detection (BFD)
IPSec имплементация	<ul style="list-style-type: none"> - 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
Брой конкурентни SSL VPN потребителя включени в системата (постоянни лицензи)	60 000 SSL VPN потребителя
Брой IPSec Site-to-Site VPN	24 000 отдалечени точки
Виртуални таблици за маршрутизация	220 броя
Поддръжка на виртуализация (виртуални контексти)	25 броя
IPv6 поддръжка	Всички конфигурации за интерфейсите 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
Брой интерфейси за управление	- 1x 1G SFP out-of-band management port - 2x 10G SFP+ интерфейси за отказоустойчивост - 1x RJ-45 конзолен порт - 1x Micro USB - Възможност за надграждане 1x 40G QSFP+ интерфейси за отказоустойчивост
Монтаж и размери	за вграждане в 19“ шкаф с максимален размер 2U
Захранване и входно напрежение	Резервирано, 100-240VAC (50-60Hz)
Функционални изисквания	<ol style="list-style-type: none"> 1) да позволява 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; 2) да анализира съдържанието за наличие на зловреден код като включва минимум AntiVirus, AntiSpyware, IPS; 3) AntiVirus инспекцията да може да задържа Zero day файл в защитната стена докато получи отговор за неговата репутация. 4) да анализира непознати заплахи (Zero Day зловреден код) в защитена среда като създава и дистрибутира сигнатури в реално време. 5) IPS да използва машинно, задълбочено обучение да открива и блокира непознати Command and Control (C2), при преминаване на непознат HTTP, HTTP2, SSL, TCP и UDP трафика през защитната стена. 6) анализът на Zero Day зловреден код трябва да използва минимум следните методи за анализ: Static Analysis, Machine Learning, Dynamic Analysis 7) да анализира PE и PowerShell скриптове в защитната стена и предоставя защита в реално време. 8) да инспектира за заплахи HTTPS протокола чрез декриптиране; 9) да инспектира за заплахи HTTP 1.1 и HTTP 2.0 протоколи; 10) 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; 11) да анализира URL и тяхното съдържание в реално време. Всяка заявка за достъп да бъде анализирана чрез Machine Learning на база на HTTP Request.

- 12) Управлението на устройството трябва да се реализира чрез физически отделени процесор, памет и интерфейси отделени от ресурсите използвани за управление на трафика.
- 13) операционната система на устройството да позволява на администратора да работи върху копие на работещата конфигурация и след като е готов с промените при потвърждение да се извърши валидация, резервно копие (backup) и прилагане на промените.
- 14) да може да дистрибутира входящите NAT сесии между няколко адреса като използва минимум следните методи: Round Robin, Source IP Hash, Least Sessions
- 15) администраторът трябва да може да изисква прекатегоризация на даден URL директно от графични интерфейс на защитната стена.
- 16) 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.
- 17) наличие на DLP (Data Loss Prevention) функционалност, за ограничаване на движението на конфиденциални файлове.
- 18) политиката за декриптиране трябва да има възможност да се настройва на база на URL или URL категория;
- 19) 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);
- 20) да изгражда отдалечен VPN достъп чрез агент инсталиран на крайно клиентската машина с Windows и MacOS .
- 21) агентът за VPN достъп трябва да поддържа (да може да бъде инсталиран) чрез добавяне на лиценз на минимум следните операционни системи: Linux, Android, iOS, Raspbian, Ubuntu.
- 22) възможност за QoS трафика според типа приложение потребител и/или URL категория;
- 23) прозрачна идентификация на потребителите от Активната директория без изискване на крайната машина да се инсталира агент, настройки в browser или отваряне на Web Portal;
- 24) да може да изпраща декриптирани потоци от данни към трети страни за допълнителен анализ след което отново да криптира трафика.
- 25) да предоставя възможност за надграждане с допълнителен лиценз за идентифициране на устройства (Device Fingerprint) в мрежата на база поведение, мета данни и логове.
- 26) да може при регистрирана атака (log) автоматично да поставя засегнатите потребители и IP в група с ограничен достъп до мрежата (изоляция или карантина);
- 27) 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.

- 28) 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).
- 29) да включва функционалност позволяваща служебния достъп до публични облачни услуги като Office 365, Google, Dropbox и YouTube, и ограничаване достъпа до лични потребителски акаунти за същите приложения.
- 30) да притежава Уеб базиран интерфейс с различни статистики на база време, приложение, категории, потребители, заплахи. Анализа на логовете и репортинг да се извършва от самото устройство чрез неговия графичен интерфейс без да е необходима инсталация на допълнителен софтуер;
- 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);
- 32) 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.
- 33) да има механизъм за откриване и превенция на DNS Tunneling канали за комуникация, включително ограничаване достъпа до автоматично генерирани домейни (Domain generation algorithms).
- 34) да открива в реално време атаки като инспектира DNS Response и DNS Request.
- 35) DNS защитата да може в реално време без допълнителни модули или платформи да прилага активна защита към специфични техники и категории като: "C&C domains", "DGA detection", "NXNSAttack", "DNS rebinding", "Malware domains", "Newly Registered Domains", "Phishing Domains", "Parked domains", "Proxy avoidance", "Ad tracking domains", "Hijacked Domains", "Misconfiguration Domains"
- 36) 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.
- 37) 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.
- 38) 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.
- 39) 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;

	<p>40) 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.</p> <p>41) да може да пропуска до три софтуерни версии при upgrade като дава възможност да изберете да пропуснете две основни версии и една второстепенна или една основна версия и две второстепенни.</p> <p>42) да има възможност да работи в режим на Explicit Proxy (PAC Files)</p> <p>43) да притежава SD WAN функционалност като покрива минимум:</p> <ul style="list-style-type: none"> - Събиране на метрики за връзката като Jitter, Latency и загуби. - Интелигентен избор на път с динамично управление на приложенията - Двупосочно измерване на пътя на трафика и прилагане на QoS - Корекция на препращането (FEC) - Корекция дублиране на пакети - Мониторинг на пътя на SaaS приложенията - Поддръжка на динамично DNS (DDNS)
Тип на поддръжката	<ul style="list-style-type: none"> - 24x7, от производителя - да се посочи продуктов номер

6. Система за съхранение на данни - 2 броя, със следните минимални технически и функционални параметри:

Параметър	Технически изисквания на възложителя
марка, модел, продуктов номер и линк към сайта на производителя	- Посочва се от участника
Общи изисквания	<ul style="list-style-type: none"> - За целите на настоящата процедура използваемото пространство за съхранение е: Пространството за съхранение, предоставяно от системата за съхранение на данни – към сървърите, след прилагане на RAID 6 защита в системата за съхранение и без прилагане на каквито и да е техники за редукция на данните (дедупликация, компресия, тънко провизиране и други). - Конфигурацията да съдържа само оригинално вложени от производителя компоненти. Не се допуска докомплектоване на дисковия масив извън фабриката на производителя. - Предложената система трябва да се достави с налични и използвани поне 48 слота слота/гнезда за устройства за енергонезависимо постоянно съхранение на потребителски данни.

	<p>Устройствата за съхранение да бъдат SSD/флаш, с NVMe интерфейс, PCI-Express поколение 4 или 5.</p> <ul style="list-style-type: none"> - Да се извършва ранно откриване на започнало злонамерено криптиране на данните в дисковия масив (т. нар. ransomware атака). - Да извършва статистически анализ в реално време на потока данни на ниво среда за съхранение с цел характеризирането му. - Да се анализират необичайни промени на ентропия, съотношение четене/запис, степен на компресиране и/или дедуплициране на данните и други метрики с цел ранна (секунди) детекция на започнала ransomware атака. - Решението да показва в кое (кои) логическо (-и) устройство (-а) в дисковия масив се случва злонамереното криптиране на данните. - Да се генерира аларма в потребителския интерфейс на решението и изпращане на ел. поща до 3 минути след като е открита атаката – в режим 24x7. - Изискването за производителност на дисковия масив да се изпълни при работеща такава функционалност. - Да се доставят всички необходими софтуерни и хардуерни продукти за реализиране на решението – да се опишат. - Ако е нужен абонамент за облачна услуга – да бъде включен в предложението за срока на поддръжка и да се опише. - Ако се ползва облачна услуга, Възложителят допуска споделяне с облака по криптирана връзка само на метаданни за дисковия масив (т. нар. телеметрия). Изпращането на същинските данни на Възложителя към трети страни е недопустимо.
Контролери	<ul style="list-style-type: none"> - Предложената дискова система да се достави с минимум една двойка контролери в конфигурация „Активен-Активен“. - Да позволява бъдещо разширение чрез изграждане на мрежа от дискови масиви с мин. 16 контролера (нода).
Памет	<ul style="list-style-type: none"> - Да се достави с минимум 1024 GB RAM cache за системата. - При аварийно спиране на захранването, подлежащите на запис данни в RAM кеш паметта да бъдат съхранени в енергийно независим носител на информация.
Пространството за съхранение	<ul style="list-style-type: none"> - да се достави с използваемо пространство за съхранение в размер на 1024.00 TiB. - пространство за съхранение да се постигне с еднакви носители на данни SSD/флаш NVMe PCI-Express поколение 4 или 5. <ul style="list-style-type: none"> - Минимум 1 брой от предложените носители на данни да бъде резервно (hot-spare) устройство за съхранение (или повече – ако добрата практика на производителя изисква повече). Допустимо е вместо посветено резервно (hot-spare) устройство за съхранение на данни, неговото пространство за съхранение да бъде разпределено измежду предложените носители на данни.
Интерфейси	<ul style="list-style-type: none"> - Да се осигурят следните портове за връзка със сървъри:

	<ul style="list-style-type: none"> - минимум по 8 порта на контролер, всеки порт 32G Fibre Channel (FC). Да поддържа NVMe over FC. Да бъдат включени по 8 броя FC 32G SW SFP модула на контролер. - минимум по 4 порта на контролер, всеки порт 25G Ethernet. Да поддържа iSCSI и IP репликация. Да бъдат включени по 4 броя Ethernet 25G SW SFP28 модула на контролер - Да се осигурява управление на дисковата система през криптирани графичен интерфейс (GUI) и команден ред (CLI). - Графичният интерфейс да показва моментни стойности на натоварването – IOPS и MB/s за четене и запис на хост сървърите; IOPS за бек-енд; времезакъснение.
Кабели	<ul style="list-style-type: none"> - Да се доставят 24 броя оптични кабели, всеки: <ul style="list-style-type: none"> - с дължина 5 метра - с LC конектори - OM3 или OM4
Резервираност	<ul style="list-style-type: none"> - Да предоставя резервиране на всички активни компоненти без единична точка за отказ - захранващ модул, контролер, носители на данни. - Да осигурява замяна на компонент (захранващ модул, батерия, контролер, носител на данни) без прекъсване на достъпа до всички данни.
Firmware	Да предоставя възможност за обновление на системния софтуер (firmware) без прекъсване на достъпа до всички данни.
Функционалности	<ul style="list-style-type: none"> - Да включва следните функционалности, лицензирани и използвани за целия инсталиран капацитет на съхранение на предложения дисков масив и за целия срок на гаранционна поддръжка: <ul style="list-style-type: none"> - Тънко провизиране (Thin Provisioning). - Инлайн дедупликация или инлайн компресия за предложените устройства за съхранение на данни. - Моментни копия (Snapshot). - Пълни локални копия (Clones). - Отдалечена асинхронна репликация по Fibre Channel и IP протоколи. - Висока наличност (High Availability) с актив-актив функционалност между двата физически дискови масива в режими четене и запис с нулево RPO между двата дискови масива.
Киберустойчивост	<p>Предложението да включва лицензирани, активирани и работещи функционалности за:</p> <ul style="list-style-type: none"> - Защитни копия на данните: <ul style="list-style-type: none"> - от вида моментна снимка (снапшот); - да не може да се монтират на сървър или ако може да се монтират, да са в режим „само четене“ (read only). - изтриването и промяната на копията да е забранено за определени роли потребители, имащи достъп до интерфейсите за

управление на дисковия масив. Само точно определени роли администратори на дисковия масив да имат права да изтриват тези копия.

- копията да се създават автоматично по политика, дефинирана само от определени (високи) роли администратори на масива. Политиката да включва избираеми от потребителя: честота на създаване на копията, времеви период на съхранение на копията, автоматично изтриване на копията след изтичане на периода.
- ако са необходими допълнителни ресурси (софтуерни продукти/лицензи, хардуерни продукти и други), за изпълнение на тези изисквания, тези ресурси да бъдат включени в предложението и да се опише действието им.
- Да има режим за администриране на дисковия масив, при който задължително да се изискват двама администратори за изпълнение на критични задачи.
- Да има пълно криптиране на всички данни на Възложителя при изпълнение на следните условия:
 - Криптирането да е от вида „в мястото на съхранение“ (т. нар. DaRe – „Data at Rest“).
 - Да се използва симетрично криптиране на данните с минимум 256-битов ключ (МЕК/DEK Media/Data Encryption Key или еквивалент съгласно технологията и терминологията на конкретния производител).
 - В случай, че МЕК/DEK се пренася по комуникационен/електронен канал извън физическата кутия на самите NVMe носители на данни, МЕК/DEK да бъде криптиран по време и в средата на преноса му до NVMe носителите на данни.
 - Предложенията да включват решение за управление на криптографските ключове така, че в енергонезависима памет вътре в дисковия масив да не се съхранява информация (ключ и/или друго), която да е достатъчна за успешно декриптиране на данните на Възложителя.
 - В случай, че изпълнението на горното изискване налага доставка на допълнителни хардуерни и/или софтуерни продукти, те да бъдат включени в предложението и да се опишат.
 - Ако се използват външни сървъри за управление на криптографски ключове, да се изгради резервирана сървърна инфраструктура от минимум два такива напълно независими сървъра така, че във всеки момент, частична или пълна загуба на данни, в който и да е от двата сървъра, да позволи успешно декриптиране на всички данни на Възложителя в дисковия масив само с използване на един работещ сървър. В този сценарий, да се предложи и независимо от сървърите решение за пълно декриптиране на всички данни на Възложителя в дисковия масив

	<p>в случай на пълен срив и пълна загуба на данните във всички сървъри за управление на криптографски ключове.</p> <ul style="list-style-type: none"> - В случай на използване на сървъри за управление на криптографски ключове, тези сървъри да не използват каквото и да е пространство за съхранение от дисковия масив, чиито криптографски ключове управляват.
<p>Софтуер за наблюдение на производителността в реално време</p>	<p>Да се достави, лицензиран за цялото предложено пространство за съхранение с включени следните функционалности:</p> <ul style="list-style-type: none"> - Снемане на отчет през времеви интервал 1 минута или по-малко за поне седем дни. - Мониторинг на производителността на Fibre Channel комутатори Broadcom/Brocade и Cisco – на ниво комутатор и на ниво порт. - Задаване на целеви стойности на избрани метрики за производителност с генериране на известия при неизпълнение на целите. - Планиране на капацитет – софтуерът да притежава аналитични функции за прогнозиране на бъдещи нужди от пространство за съхранение към избрана дата. - Да съхранява информацията за една година назад (допуска се това да бъде с намалена гранулярност на статистическите данни). - Описаните функционалности да се постигнат в локална (необлачна, on-premise) софтуерна среда.
<p>Телеметрия</p>	<p>Да се предостави телеметрична услуга от облачната среда на производителя на дисковия масив. Услугата да включва следните функционалности за отдалечено наблюдение и поддръжка на системата за съхранение:</p> <ul style="list-style-type: none"> - Графичен потребителски интерфейс (GUI). - Инвентаризация на дисковия масив и отчети за използвания капацитет за съхранение. - Мониторинг на капацитет за съхранение – използван, наличен, спестен чрез редукция на данните. - Запазване на данните за конфигурацията и капацитета за повече от една година. - Бързо изолиране на проблемни събития. - Изпращане на аларми, предсказващи проблеми. - Мониторинг на изправността с функция call home. - Отваряне и управление на заявки за поддръжка (tickets) към производителя. - Събиране и изпращане на журнали (лог файлове) за машината към производителя – от интерфейса на облачната услуга. <p>Всички функционалности да са достъпни през облачно базиран интерфейс на услугата.</p> <ul style="list-style-type: none"> - Ако е необходима сървърна машина за комуникиране на телеметричните данни от дисковия масив към облака, тази

	машина (с всичките ѝ хардуерни и софтуерни компоненти) да бъде включена в предложението и да се опише.
Съвместимост	С цел постигане на максимална свобода при избор на софтуерни платформи за приложения, дисковият масив да е съвместим с най-масово използваните операционни системи, среди за сървърна виртуализация и среди за управление на контейнерни приложения с утвърдените им популярни версии: Microsoft Windows Server 2022; Red Hat Enterprise Linux® 9.4; CSI драйвър за Red Hat OpenShift 4.18; Ubuntu 22.04, CSI драйвър за Kubernetes 1.32, SUSE Linux Enterprise Server 15 SP6; VMware® vSphere/ESXi 8.0 U3.
Крепежи	Да се доставят всички необходими крепежни елементи, монтажни комплекти, захранващи кабели, мрежови кабели, оптични кабели както и лицензи, необходими за изпълнение на всички изисквания и за пълноценно функциониране на дисковата система.
Тип на поддръжката	<ul style="list-style-type: none"> - 24x7, от производителя, за хардуера и софтуера, с включено право да се ползват без допълнително заплащане поправки и нови версии на софтуера за целия срок на поддръжката. - Включена отдалечена техническа поддръжка от производителя в режим 24x7.

7. Сървърна система – 1 брой, със следните минимални технически параметри:

Параметър	Технически изисквания на възложителя
марка, модел, продуктов номер и линк към сайта на производителя	Посочва се от участника
Свързаност	Сървърната система трябва да поддържа едновременната работа на минимум 160 блейд и рак сървъри.
Свързаност	Сървърната система трябва да включва две устройства работещи в клъстър, които осигуряват мрежовата свързаност на сървърите и се управляват от същата система, от която и сървърите.
Свързаност	<p>Устройствата за мрежова свързаност трябва да притежават минимум следните портове:</p> <ul style="list-style-type: none"> - 32 QSFP порта, които поддържат: <ul style="list-style-type: none"> ✓ 40/100Gbit/s Ethernet или FCoE ✓ 10/25Gbit/s Ethernet чрез breakout или QSFP към SFP адаптер - 4 QSFP порта, които поддържат: <ul style="list-style-type: none"> ✓ 40/100Gbit/s Ethernet или FCoE ✓ 10/25Gbit/s Ethernet чрез breakout или QSFP към SFP адаптер ✓ Разцепване на всеки порт на 4 x 8/16/32Gbit/s FC порта
Свързаност	Устройствата за мрежова свързаност трябва да притежават line-rate производителност.

Свързаност	Устройствата за мрежова свързаност трябва да поддържат минимум 2000 VLAN-а.
Свързаност	Устройствата за мрежова свързаност трябва да притежават резервирани hot-swappable вентилатори и захранвания
Свързаност	Устройствата за мрежова свързаност трябва да притежават всички нужни за тази инсталация лицензи.
Свързаност	Устройствата за мрежова свързаност трябва да поддържат 100Gbit/s трафичен поток (single-flow)
Свързаност	Устройствата за мрежова свързаност трябва да поддържат: <ul style="list-style-type: none"> - PFC (per-priority pause frame support) - IEEE 802.1Qaz - IEEE 802.3ad - IEEE 802.3x - IEEE 802.1Q - Layer 2 IEEE 802.1p - IEEE 802.1w - Remote Network MONitoring (RMON) - Weighted Round-Robin (WRR) QoS - IGMP v1,v2,v3 snooping - Jumbo frame 9216 bayts - Откриване на slow drain в FC/FCoE. - Размер не по-голям от 1RU
Свързаност	Към всяко устройство за мрежова свързаност трябва да бъдат доставени следните QSFP/SFP: <ul style="list-style-type: none"> - За връзка към шаситата: <ul style="list-style-type: none"> ✓ 8 x MMF QSFP 100Gbit/s работещи на минимум 100 м. - За връзка към Ethernet Мрежата <ul style="list-style-type: none"> ✓ 4 x MMF QSFP 100Gbit/s работещи на минимум 100 м. - За връзка към FC Мрежата <ul style="list-style-type: none"> ✓ 2 x QSFP 4x32Gbit/s breakout
Управление и наблюдение	<ul style="list-style-type: none"> - Сървърната система трябва да включва единна платформа за конфигуриране, управление(мениджмънт) и наблюдение доставена от производителя. - Платформата трябва да използва Redfish базиран стандартен модел за управлението на устройствата и сървърите. Платформата трябва да поддържа rack-сървъри и блейд сървъри. - Всички доставени сървъри трябва да са лицензирани.
Управление и наблюдение	<ul style="list-style-type: none"> - Платформата за управление трябва да поддържа конфигурирането на сървърните характеристики чрез профили. - Профилите трябва да позволяват дефинирането на следните параметри: <ul style="list-style-type: none"> ✓ BIOS Settings ✓ Boot Order

	<ul style="list-style-type: none"> ✓ Колко vNIC-а ще се предоставят на OS и как ще бъдат конфигурирани. <ul style="list-style-type: none"> • vNIC VLAN settings <ul style="list-style-type: none"> ▪ VLAN IDs ▪ Access или Trunk ▪ Native VLAN • vNIC Ethernet QoS <ul style="list-style-type: none"> ▪ Class of Service на излизания от vNIC трафик. ▪ MTU ▪ Burst Rate • vNIC функционалности –NVGRE, VXLAN, Interrupt, RoCE, и TCP Offload настройки. • VMMQ ✓ Колко vHBA-а ще са предоставят на OS и как ще бъдат конфигурирани. ✓ vHBA QoS configuration <ul style="list-style-type: none"> • System class на излизания от vHBA трафик • Maximum Data Field • Burst Rate ✓ iSCSI Boot ✓ LDAP configuration settings ✓ SMTP Policy ✓ SOL Policy ✓ SSH Policy ✓ IPMI Policy ✓ SNMP Policy ✓ Syslog Policy ✓ Virtual KVM Policy ✓ Virtual Media Policy ✓ MAC addresses ✓ WWNN address ✓ WWPN address ✓ M.2 RAID конфигурация ✓ RAID конфигурация
Управление и наблюдение	Платформата за управление трябва да поддържа конфигурирането на QinQ (802.1Qin802.1Q)
Управление и наблюдение	Платформата за управление трябва да поддържа събирането и показването на следните статистики: консумирана енергия от сървърите, количество Correctable и uncorrectable в паметите, температура, натоварване на процесори, натоварване на паметта, количество трафик TX/RX и грешки по интерфейсите виртуални и физически в системата.
Управление и наблюдение	Платформата за управление трябва да поддържа обновяването на firmware-ите на устройства, сървъри и компоненти на шасита.

Управление и наблюдение	Платформата за управление трябва да поддържа наблюдение на състоянието на всеки сървър свързан с нея.
Управление и наблюдение	Платформата за управление трябва да поддържа клониране на сървърни профили.
Управление и наблюдение	Платформата за управление трябва да поддържа темплейти на сървърни профили.
Управление и наблюдение	Платформата за управление трябва да поддържа генерирането и събирането на логове нужни при отстраняването на неизправности в системата.
Управление и наблюдение	Платформата за управление трябва да поддържа dashboard за всички свързани устройства и сървъри, които да може да се персонализира от потребителя.
Управление и наблюдение	Платформата за управление трябва да поддържа функционалност за автоматична проверка дали комбинацията сървърен хардуер, сървърен firmware, операционна система и драйвери се поддържа официално от производителя (HCL).
Управление и наблюдение	Платформата за управление трябва да поддържа проверка дали някой от елементите на системата е засегнат от проблем със сигурността публикуван от производителят (CVE). Платформата трябва да предостави информация, информация за проблема, кои са засегнатите устройства, и workaround/решение.
Управление и наблюдение	Платформата за управление трябва да поддържа автоматичната проверка дали някой от елементите на системата е засегнат от значим проблем не свързан със сигурността публикуван от производителя.
Управление и наблюдение	Платформата за управление трябва да поддържа тагване на елементи.
Управление и наблюдение	<p>Платформата да може да събира следните параметри и да пази информацията минимум 90 дни:</p> <ul style="list-style-type: none"> - Мрежови статистики на ниво vNIC/vHBA: <ul style="list-style-type: none"> ✓ Изпратен трафик(количество и брой пакети); ✓ Получен трафик(количество и брой пакети); ✓ Получени пакети със CRC грешки; ✓ Натовареност на интерфейс в посока изпращане; ✓ Натовареност на интерфейс в посока получаване; - Поправими ECC грешки. - Непоправими ECC грешки. - Температура. - Консумирана електро енергия.
Блейд шаси	Количество: 2 бр.
Блейд шаси	Шасито не трябва да има midplane. Блейдовете се включват директно в I/O модулите.
Блейд шаси	Шасито да не е по-голямо от 7RU

Блейд шаси	Шасито трябва да поддържа минимум 8 блейда.
Блейд шаси	Шасито трябва да има hot-swappable вентилатори.
Блейд шаси	Шасито трябва да включва поне 2 модула, които предоставят Ethernet, FCoE и мениджмънт свързаност. Всеки модул да отговаря ва следните изисквания: <ul style="list-style-type: none"> - Минимум 8x100Gbit/s QSFP външни портове - Минимум 100Gbit/s към всеки блейд сървър - Не трябва да комутира между блейдове - Трябва да поддържа 100Gbit/s трафичен поток (single-flow) .
Блейд шаси	Шасито не трябва да има модул преназначен само за управление
Блейд шаси	Шасито трябва да бъде окомплектовано с всички захранвания.
Блейд шаси	LAN, SAN и трафика за управление трябва да използват едни и същи портове.
Блейд сървъри	Блейд сървъри / Количество:16 бр.
Блейд сървъри	CPU: <ul style="list-style-type: none"> - Количество: 2 - Минимална честота: 2.2 GHz - Минимален брой ядра: 36 - Минимален резултат от SPECrate@2017_int_base: 650
Блейд сървъри	Минимум памет: 1024 GB (16*64GB) минимум DDR5-5600Mhz
Блейд сървъри	Дискове: <ul style="list-style-type: none"> - M.2 RAID Контролер - M.2 2x480 GB SSD
Блейд сървъри	I/O адаптер със следните минимални характеристики: <ul style="list-style-type: none"> - Трябва да поддържа минимум 2 x 100-Gbit/s Ethernet connections. - Трябва да поддържа FCoE. - Трябва да поддържа 100Gbit/s трафичен поток (single-flow) . - Трябва да поддържа създаването на минимум 128 виртуални мрежови адаптера (vNICs и vHBAs) без да се използва SR-IOV. - Трябва да поддържа DPDK, iSCSI, iSCSI Boot, NPIV, usNIC, VMQ/VMMQ, VXLAN/NVGRE, IEEE 802.3x, IEEE 802.1q, IEEE 802.1p, IEEE 802.1Qaz, IEEE 802.1Qbb, SCSI-FCP, RoCEv2. - Should support performance of at least 800000 IOPS
Блейд сървъри	Да бъде включен TPM 2.0
Гаранция и поддръжка	<ul style="list-style-type: none"> - Тип 24x7x4 за предложения срок на поддръжка (минимум 3 години) - Получаване на нови версии на софтуера за периода на поддръжка - Срок на абонаментите за използване на софтуерни функции за периода на поддръжка

8. SDN за център за данни - 1 брой, със следните минимални технически параметри:

Параметър	Технически изисквания на възложителя
марка, модел, продуктов номер и линк към сайта на производителя	Посочва се от участника
Шаси/кутия и захранване	Всички устройства трябва да позволяват директен монтаж в 19“ шкаф.
Шаси/кутия и захранване	Всички устройства трябва да имат минимум два токозахранващи модула, работещи в режим с пълно резервиране. Да поддържат захранване от 220-240v AC, 50Hz.
Шаси/кутия и захранване	Всички устройства трябва да имат минимум един 10/100/1000BASE-T и един сериен интерфейс (конзола) за управление (OOB).
Шаси/кутия и захранване	Всички устройства трябва да имат минимум един USB порт.
Основни функции	Предложеното решение за SDN (Software Defined Network) трябва да включва следните компоненти: <ul style="list-style-type: none"> - Резервиран клъстер от минимум три контролера. - Фабрика от два опорни (Spine) комутатора и два крайни (Leaf) комутатора. - Опорните комутатори трябва имат минимум тридесет и два 100/400 Gbit/s QSFP-DD. - Крайните комутатори трябва да имат минимум четиридесет и осем 1/10/25 Gbit/s SFP28 и шест 40/100 Gbit/s QSFP28 интерфейса.
Основни функции	За връзки между комутаторите(Spine-Leaf) трябва да се осигурят следните трансивери съвместими с тях: <ul style="list-style-type: none"> - 8 x MMF QSFP 100Gbit/s работещи на минимум 100 м.
Основни функции	За връзки между комутаторите и контролерите трябва да се осигурят следните трансивери: <ul style="list-style-type: none"> - 10Gbit/s DAC SFP+ кабел с дължина 3 метра – 6 броя.
Основни функции	Всички хардуерни и софтуерни компоненти на решението трябва да са от един производител.
Основни функции	Всички комутатори трябва да имат неблокируема архитектура.
Основни функции	Комутаторите трябва да поддържат Spine/Leaf топология на две нива.
Основни функции	Предложеното решение трябва да е напълно резервирано. Работа на системата трябва да продължи при отпадане на който и да е единичен компонент като предлага бързо възстановяване.
Основни функции	Отпадането или добавяне на контролер не трябва да нарушава работата на системата. Отпадането дори на всички контролери не трябва да спира работата на вече провизирани услуги.
Основни функции	Решението трябва да поддържа IPv4 и IPv6.

Основни функции	Опорните комутатори и крайните комутатори трябва да имат възможност за добавяне директно или чрез допълнителен лиценз на IEEE 802.1ae. Като всеки комутатор трябва да има минимум 8 порта, които поддържат IEEE 802.1ae със скорост wire-rate.
Основни функции	Всеки краен комутатор трябва да е закачен към всеки от опорните комутатори посредством 100 Gbps връзка. Да се предвидят необходимите трансивери. Трябва да се поддържат разстояния в рамките на два съседни комуникационни шкафа.
Основни функции	Предложеното решение трябва да позволява увеличаване на производителността чрез добавяне на Spine комутатори (до шест броя общо).
Основни функции	Предложеното решение трябва да позволява увеличаване на капацитета чрез добавяне на Leaf комутатори (до двадесет и четири броя от предложеният тип общо).
Основни функции	Предложеното решение трябва да позволява добавяне или премахване на компоненти от фабриката (контролери, комутатори) без прекъсване на услугите.
Основни функции	Предложеното решение трябва да поддържа технология за виртуализация на мрежата - VxLAN.
Основни функции	Предложеното решение трябва да поддържа технология за разтегляне на Layer 2 VLAN мрежи между два и повече центъра за данни, позволявайки миграция на сървъри и виртуално машини без промяна на адресната им схема.
Основни функции	Мрежовата архитектура трябва да е поддържа "VxLAN overlay" в хардуера за да осигурява логически топологии и абстракция на хардуера без загуба на производителност.
Основни функции	Решението трябва да поддържа "multi-home" и "multi-pathing" при бъдещо разширение към допълнителни центрове за данни за ефективно използване на капацитета на всички активни връзки.
Основни функции	Решението трябва да поддържа отдалечени крайни комутатори през IP свързаност. Трябва да се поддържат до пет подобни инсталации.
Основни функции	Решението трябва да позволява разширение до пет центъра за данни с добавяне единствено на комутатори и без допълнителна инвестиция за контролери.
Основни функции	Решението трябва да позволява връзка към други фабрики/кълъстери с възможност за централизирано управление.
Основни функции	Решението трябва да притежава средства за контрол на BUM (broadcast, unknown unicast, multicast) трафика.
Основни функции	Решението трябва да позволява интеграция с L4-7 устройства (защитни стени, IPS/IDS-и, loadbalancer-и).
Основни функции	Решението трябва да позволява интеграция със защитни стени в „transparent” или „routed” режим изпълнени както със хардуер така и виртуални.

Основни функции	Решението трябва да позволява интеграция с хипервайзори на Vmware, Microsoft и Redhat, Nutanix.
Основни функции	Трафика от виртуални машини и физически сървъри трябва да подлежи на идентичен контрол.
Основни функции	Решението трябва да поддържа провизиране и наблюдение на порт групи на виртуални машини на различни хипервийзори (Vmware ESXi, Nutanix, Red Hat OpenShift).
Основни функции	Решението трябва да наблюдава и визуализира чрез контролера загуби на пакети и закъснения.
Основни функции	Фабриката трябва да балансира автоматично трафика с пренасочване към по-слабо натоварени връзки при задръстване.
Основни функции	Фабриката трябва да приоритизира по-леките потоци от информация за сметка на по-тежките.
Основни функции	Решението трябва да поддържа дистрибутиран шлюз по подразбиране (default gateway) на всеки краен комутатор. Ако е необходима маршрутизация тя трябва да се извършва още на първият комутатор от фабриката където влиза трафика.
Основни функции	Решението трябва да поддържа множество връзки към външни мрежи с поддръжка на BGP, OSPF и статична маршрутизация. Трябва да се поддържат филтри (префикс листи) входящо и изходящо от фабриката.
Основни функции	Научаването на MAC, IP, VTEP ID, трябва да става хардуера на фабриката с цел по-добра производителност.
Основни функции	Решението трябва да поддържа DHCP relay.
Основни функции	Решението трябва да поддържа изолация на сървъри в един мрежов сегмент независимо дали са физически или виртуални.
Основни функции	Решението трябва да поддържа списъци за контрол на достъпа (ACL) между сървъри или група независимо дали са физически или виртуални.
Основни функции	Решението трябва да поддържа хостове закачени към два различни комутатора за резервиране чрез MCEC (Multi-chassis etherchannel) технология. Трябва да се поддържа LACP протокол.
Управление и наблюдение	Цялата фабрика трябва се де менажира като един логически компонент.
Управление и наблюдение	Клъстера от контролери трябва да се синхронизира автоматично. Трябва да притежава решение при евентуален „split-brain” сценарий.
Управление и наблюдение	Решението трябва да позволява логическо разделение на системата между различни ползватели (multi-tenant) със напълно самостоятелна политика. Трафик между различни ползватели (tenants) трябва да е възможен само по контролиран път през защитни стени.

Управление и наблюдение	Решението трябва да позволява автоматизирано (zero-touch) провизиране на комутатори.
Управление и наблюдение	Решението трябва да поддържа автоматично откриване на топологията на фабриката по LLDP и визуализирането и през контролерите.
Управление и наблюдение	Решението трябва да е програмируемо със възможност за промени през отворен програмен интерфейс (API). Достъпа до API трябва да е ограничен единствено през една точка (клъстера от контролери). Трябва да могат да се поддържат оркестратори и системи за управление на други производители.
Управление и наблюдение	Решението трябва да поддържа SNMP протокол.
Управление и наблюдение	Решението трябва да поддържа TACACS+, RADIUS, LDAP и локална автентикация. Решението трябва да може да се интегрира с активна директория посредством LDAP протокол.
Управление и наблюдение	Решението трябва да поддържа роли ограничаващи достъпа на потребителите на системата само до определени функции.
Управление и наблюдение	Решението трябва да поддържа двуфакторна автентикация.
Управление и наблюдение	Решението трябва да поддържа автоматично провизиране на услуги през RESTful API в JSON и XML формат.
Управление и наблюдение	Фабриката трябва да поддържа различни опции за програмируемост: python, bash, netconf, xml/json.
Управление и наблюдение	Доставчикът трябва да осигури безплатно симулатор на софтуера на контролера (виртуална машина или хардуер) който може да се използва за тестове и обучение.
Управление и наблюдение	Комутаторите трябва да поддържат CLI интерфейс за мониторинг и откриване на проблеми.
Управление и наблюдение	Контролерът трябва да запазва конфигурацията на регулярни интервали или при команда и да може да възстановява стара такава при необходимост.
Управление и наблюдение	Да се включи софтуер за мониториране на системата след първоначална инсталация (Day 2 Ops) за проактивно откриване и отстраняване на проблеми в системата. Да поддържа проверка дали някой от елементите на системата е засегнат от проблем със сигурността публикуван от производителя. Да предупреждава, ако софтуерен или хардуерен елемент ще е end-of-support следващите 12 месеца.
Управление и наблюдение	За връзки с външни за фабриката устройства трябва да се осигурят следните трансивери: 10Gbit/s SR SFP+ – 8 броя.
Гаранция и поддръжка	- Тип 24x7x4, техническа поддръжка директно от производителя и включените абонаменти за периода на поддръжка (минимум 3 години)

	- Получаване на нови версии на софтуера за периода на поддръжка.
--	--

9. FC комутатори - 2 броя, със следните минимални технически параметри:

Параметър	Технически изисквания на възложителя
марка, модел, продуктов номер и линк към сайта на производителя	Посочва се от участника
Общо изискване	да е фиксиран, с размер не по голям от 1RU притежаващ минимум 32 порта или 16 порта с възможност за разширяване до 32 порта.
Портове	да бъде доставен с не по-малко от 16 бр. активирани FC порта, поддържащи 4/8/16/32Gbit/s.
SFP модули	да бъде доставен с 16 бр. 32 Gbit/s SFP работещи по MM влакно на разстояние поне 300 метра.
SFP модули	да поддържа 32Gbit/s, 16Gbit/s и 8Gbit/s SFP-та.
Производителност	да притежава производителност, позволяваща едновременната работа на всички портове на комутатора със скорост 32Gbit/s.
Функционалност	да има възможност, чрез лицензиране да поддържа 128bit AES криптиране на трафика на поне 4 порта със скорост 32Gbit/s. Пускането на тази функционалност да не води до загуба на буфер кредити, портове или друга функционалност на комутатора.
Функционалност	да има възможност, чрез лицензиране да поддържа експорта на информация/телеметрия за минимум 10000 ITL/ITN трафични потоци, която да включва Initiator ID, Target ID, LUN/NSID свързани с target-та, IOPS/s, големина на трафичните потоци за писане и четене, Exchange Completion Time, Data Access Latency, Outstanding IO, брой на настъпилите грешки.
Функционалност	да има възможност, чрез лицензиране да поддържа конфигурирането на порт с минимум 8000 буфер кредита.
Функционалност	да поддържа автоматично зонироване на initiators и targets и автоматичното добавяне на нови зони при добавяне на initiator или target.
Функционалност	да позволява обединяването на поне 16 физически линка в един логически с обща скорост от минимум 512Gbit/s.
Функционалност	да поддържа secure boot.
Функционалност	да поддържа in-band управление чрез IP върху FC.
Функционалност	да поддържа разделяне на мрежата на минимум 4 виртуални SAN мрежи.
Функционалност	да поддържа REST API.
Функционалност	да може да се вгради в 19 инчов Electronic Industries Alliance (EIA) rack

Захранване и охлаждане	да бъде доставен с резервирани захранващи блокове и вентилатори модули.
Захранване и охлаждане	Захранващите кабели да са тип C14-C15
Захранване и охлаждане	да е с въздушен поток с изход при портовете.
Работна среда	да може да работи при температури от 10 до 30 C
Работна среда	да може да работи при влажност от 10 до 90%
Функционалност	да поддържа обновяване на софтуера без прекъсване в работата.
Функционалност	да поддържа SSHv2.
Функционалност	да поддържа отговора на команди да е във XML или JSON формат.
Регулаторни изисквания	да отговаря на следните регулаторни изисквания: - EN55022 Class A - EN55024 - EN50082-1 - EN61000-3-2 - EN61000-3-3 - EN61000-6-1 - EN 60950"
Гаранция и поддръжка	Тип 24x7x4 поддръжка от производителя на всички хардуерни и софтуерни компоненти за предложения период на поддръжка (мин. 3 години)

10. Аксесоари за 2 броя сървърни 19" 48U (600 x 1000 x 2259 мм) шкафа, със следните минимални технически параметри:

Параметър	Технически изисквания на възложителя
Токоразпределителни модули (PDU) - хоризонтални	1U, с шуко гнезда, за монтаж в сървърен шкаф 19" 48 U (600 x 1000 x 2259). Броят на модулите и гнездата се определя от участника съобразно изискванията за инсталация на предложеното оборудването.
Токоразпределителни модули (PDU) - вертикални	1U, с C13/C19 конектори, за монтаж в сървърен шкаф 19" 48 U (600 x 1000 x 2259). Броят на модулите се определя от участника съобразно изискванията за инсталация на предложеното оборудването.
Кабелни аранжори - 8 броя	Кабелни аранжори с метални скоби с подходяща дълбочина

Забележки:

1. Устройствата, предмет на доставката, трябва да съответстват или да надвишават в техническо отношение посочените минимални изисквания в Техническото задание.

2. Всеки участник посочва марка, модел, продуктово номер и линк към сайта на производителя на предлаганото устройство и софтуер и линк към сайта на производителя за доказване на съответствие с минималните изисквания.

3. Навсякъде в Техническото задание, където се съдържа посочване на конкретен модел, източник, процес, търговска марка, патент, тип, произход, стандарт или производство да се чете и разбира „или ЕКВИВАЛЕНТ“. В случай на предоставяне на еквивалент, Участникът следва да докаже, че предлаганите решения удовлетворяват по еквивалентен начин изискванията, определени от техническата спецификация.

III. ДОПЪЛНИТЕЛНИ ИЗИСКВАНИЯ:

1. Изпълнителят, следва да осигури всички необходими съпътстващи изпълнението - дейности по внедряване и пускане в експлоатация на доставеното оборудване и софтуер:

- Физическа инсталация на доставените хардуерни устройства;
- Инсталация на доставеното оборудване и софтуер за работа в инфраструктурата на Възложителя;
- Настройки на функционалности, политики и правила на доставените софтуерни и хардуерни системи;
- Конфигуриране и тестване за работоспособност;
- Внедряване на доставеното оборудване и софтуер;
- Провеждане на обучение на до 3-ма служителя на Възложителя за администриране, обслужване и експлоатация на внедреното оборудване, с продължителност до 40 часа.
- При необходимост от смяна на локацията на Възложителя в периода на гаранционна поддръжка, в който е внедрено доставеното оборудване и софтуер, ангажимент на Изпълнителя е да премести оборудването в нова локация, посочена от Възложителя, и пусне в експлоатация същото.

2. Да осигури необходимото качество на услугите по възстановяване на системи и инфраструктура при възникнала необходимост за срока на договора, по условията на т. 5 от Техническото задание;

3. При възникнала трудност в процеса на интеграция на решението по предоставяне на DR услуги, Изпълнителят е длъжен да уведоми писмено Възложителят и да предложи вариант за отстраняването му с конкретни срокове за изпълнение.