ЗАЯВКА по Рамков договор № РД-14-40 от 29.05.2023 г. (вх. № ПО-16-2224/29.05.2023 г. на „Информационно обслужване“ АД)	☒
ЗАЯВКА по Рамков договор № РД-14-40 от 29.05.2023 г. (вх. № ПО-16-2224/29.05.2023 г. на „Информационно обслужване“ АД) (актуализирана)	☐ [1]

Позиция от ПГ-2026 г.:	*№ по ред от ПГ*	*25*
Описание на проект съгласно ПГ:	*Надграждане на инфраструктурата на НЗОК, проект на части*	
CPV код	*48218000-9*	
Рег. номер на писмо от МЕУ за утвърждаване на проекта /становище по проекта	*Рег. № 92-00-753/04.11.2026 г.*	
Изискване за достъп до класифицирана информация ДА/НЕ	*Не*	

Стойност: (*стойността следва да съответства на заложената в План-графика***) без ДДС***, в т.ч. разбивка на стойността за проекти на части/ с акредитив/ авансово*	*Общо 204 740,00 евро без ДДС, от които:* *Дейност 1 – 92 280,00 евро без ДДС* *Дейност 2 – 112 460,00 евро без ДДС*
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*	*На части, с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на всяка извършена доставка/услуга по съответната дейност и издадена фактура.*
Плащане с акредитив или авансово ДА/НЕ	*НЕ*
Документи за плащане с акредитив или авансово	*неприложимо*
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*Срок за осигуряване - до 4 месеца след подписване на заявката.* *Срок на поддръжка:* *Дейност 1 - 36 месеца от осигуряване* *Дейност 2 – 60 месеца от осигуряване*
Гаранционен срок: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*неприложимо*
Отчитане: *(периодично – посочва*	*На части, след подписване на приемо-*

[1] Отбелязва се в случай че заявката е актуализирана

се период, еднократно, срок за отчитане, отчетни документи)	*предавателен протокол по чл. 6 от договора, удостоверяващ приемане на всяка извършена доставка/услуга по съответната дейност.*
Приложения: (*напр: технически параметри, образци на отчетни документи*)	*Технически параметри*
Настоящата заявка да се изпълни при условията на приложените Технически параметри.	
ЗАЯВКАТА е ИЗГОТВЕНА ОТ:	
Ръководител на проект по заявката от страна на БЕНЕФИЦИЕРА (напр: представител на дирекцията – Заявител):	*Подпис:*
ЗАЯВКАТА е ОДОБРЕНА ОТ:	
Координатор на договора от страна на ВЪЗЛОЖИТЕЛЯ:	*Подпис:*
Ръководител на договора от страна на БЕНЕФИЦИЕРА:	*Подпис:*
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:	

Ръководител на проект по заявката	*Подпис:*
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД	*Подпис:*

Забележка: *С една заявка могат да се възлагат повече от един проект по ПГ, само когато те са еднотипни и управлението им (възлагане, изпълнение, отчитане) може да се извършва съгласно описаните в таблицата от заглавната страница на заявката параметри и лица. В този случай в таблицата се добавят необходимия брой редове, за описване на съответните проекти. Когато проектите не са еднотипни, те се възлагат с отделни заявки.*

Заличаванията в документите са на основание чл. 4 от Общия регламент относно защитата на данните - Регламент (ЕС) 2016/679

ТЕХНИЧЕСКИ ПАРАМЕТРИ

за

„Надграждане на инфраструктурата на НЗОК, проект на части“

В предмета на заявката „Надграждане на инфраструктурата на НЗОК“ се включват следните дейности:

- Дейност 1 - Осигуряване на лицензи за софтуер за архивиране за срок от 3 години.
- Дейност 2 - Осигуряване на web application firewall за срок от 5 години.

2. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО

Минималните изискванията на Бенефициера относно обхвата и изпълнението на дейностите по надграждане на инфраструктурата на НЗОК, са както следва:

2.1 Минимални изисквания за дейност 1 – „Осигуряване на лицензи за софтуер за архивиране за срок от 3 години“

Целта на дейност 1 е осигуряване на лицензи за софтуер за архивиране, със следните минимални технически изисквания:

Минимални технически изисквания	
REQ.1	Предложеното решение трябва да включва лиценз за софтуер за архивиране за минимум 200 виртуални сървъра/гост операционни системи и отделен минимум от 50 TB front-end лицензиран капацитет, различен от лицензирането на виртуални сървъри/гост операционни системи, за защита на невиртуализирани работни натоварвания, включително файлови системи, приложения и бази данни.
REQ.2	Предложеното решение трябва да бъде цялостно решение за защита на данните, поддържащо всички основни операционни системи, приложения и бази данни както на виртуални, така и на физически сървъри, NAS споделени ресурси и облачна инфраструктура, включително поддръжка на множество методи за защита като архивиране и съхранение, управление на моментни снимки (snapshots), репликация и индексиране на съдържанието за eDiscovery.
REQ.3	Предложеното решение трябва да включва централизирана уеб-базирана унифицирана конзола за администриране, конфигуриране, мониторинг и отчитане на всички задачи по управление на данни в предприятието. Конзолата трябва да включва табла (dashboards) за управление и интерактивни съветници (wizards), включително прегледи и отчети за състоянието на сигурността.
REQ.4	Предложеното решение трябва да има ефективни възможности за управление на съхранението, използвайки вградена дедупликация и компресия с поддръжка на: a) Дедупликация от страна на клиента b) Дедупликация от страна на сториджа c) Глобална дедупликация, която премахва излишните копия на данни между различни резервни копия
REQ.5	Предложеното решение трябва да се интегрира с технологиите за хардуерни моментни снимки на водещите в индустрията системи за съхранение и да автоматизира създаването на индексирани, application-aware хардуерни моментни

Минимални технически изисквания	
	снимки (snapshots) в среди изградени със системи за съхранение на данни от разнообразни доставчици, с пълна съвместимост с приложения за критични Oracle и SQL среди, включително автоматизирана оркестрация на моментните снимки с глобална дедупликация и компресия.
REQ.6	Предложеното решение трябва да осигурява единен интерфейс за политики, архивиране и възстановяване на виртуални машини, физически сървъри, бази данни и Kubernetes приложения, включително мониторинг и отчетност по REQ.3 и REQ.19, с общи роли и права за достъп. Не се допускат отделни продукти със собствено управление или административна конзола, включително интегрирани чрез plug-in.
REQ.7	Предложеното решение трябва да поддържа операции по архивиране и възстановяване за следните хипервайзори и други, без необходимостта от агенти: VMware vSphere Microsoft Hyper-V Nutanix Acropolis Hypervisor (AHV) Oracle VM OpenStack RHEV Citrix XenServer
REQ.8	Предложеното решение трябва да поддържа операции по архивиране и възстановяване за следните облачни виртуални машини и други, без необходимостта от агенти: Microsoft Azure Amazon Web Services Google Cloud Platform Alibaba Cloud Oracle Cloud
REQ.9	Предложената архитектура на решението трябва да бъде базирана на трислойна архитектура, състояща се от следните функционални компоненти: a) Сървър за управление – координира всички операции по архивиране и възстановяване и съхранява в своя база данни конфигурацията, настройките за сигурност и историята на операциите. b) Медийни сървъри – пренасят архивните данни към хранилищата и управляват дисковите, лентовите и облачните хранилища, свързани към тях. c) Клиенти – агенти и/или прокси компоненти, които осигуряват защитата и преноса на данни за съответните защитавани натоварвания.
REQ.10	Предложеното решение трябва да може да реализира архив върху физически и виртуални лентови устройства.
REQ.11	Предложеното решение трябва да може да изпълнява автоматично рестартиране на задачи и да осигури функции за валидиране на данните, за да гарантира тяхната цялост чрез проверка по време на архивиране, когато данните са в покой и по време на операциите за копиране на данни.
REQ.12	Предложеното решение трябва да поддържа пълно, инкрементално, диференциално, синтетично пълно и блоково архивиране, непрекъсната инкрементална защита (Incremental Forever) и технологията Change Block Tracking (CBT). Синтетичните пълни архиви трябва да се създават чрез консолидиране на данни от последното пълно или синтетично пълно архивиране и последващите инкрементални архиви, вместо чрез четене на данните от клиентския компютър.
REQ.13	Предложеното решение трябва да позволява пълно и частично/гранулярно възстановяване на обекти от архивните данни, включително възстановяване на

Минимални технически изисквания	
	образи и гранулирано възстановяване от архиви на ниво образ, възстановяване на данни към определен момент във времето и възстановяване на същото или на друго местоположение.
REQ.14	Предложеното решение трябва да поддържа автоматично създаване на вторични копия, да позволява отложено създаване на допълнителни копия и дефиниране на различни периоди на съхранение за всяко вторично копие.
REQ.15	Предложеното решение трябва да поддържа оптимизирано създаване на вторично копие на отдалечен сайт в дедуплициран формат, където през мрежата се изпращат само уникалните блокове от данни, и безпроблемно възстановяване от спомагателното копие, в случай че основното копие не е налично.
REQ.16	Предложеното решение трябва да поддържа следните възможности за репликация: Блоково ниво репликация Репликация на база данни Периодична репликация Непрекъсната репликация Мониторинг на репликация Репликация на моментни снимки Репликация на виртуални машини
REQ.17	Предложеното решение трябва да поддържа: a) Физическо към виртуално възстановяване b) Виртуално към физическо възстановяване c) Възстановяване на хардуерно ниво (Bare metal) d) Виртуално към виртуално възстановяване между различни хипервайзори, включително преобразуване на виртуални машини (Cross-Hypervisor conversion) без използване на допълнителни инструменти (SW/HW), като при възстановяване администраторът избира хипервайзора, с който да използва виртуалната машина.
REQ.18	Решението да позволи централизирано управление чрез гъвкав потребителски интерфейс, централизирано прилагане на политики за сигурност и одит, включително криптиране, контрол на достъпа и разделяне на ролите.
REQ.19	Предложеното решение трябва да предоставя детайлни отчети, включително изпълнителни табла за управление, анализ на данните и прогнози за капацитет.
REQ.20	Предложеното решение трябва да осигурява вградено криптиране на данните както в покой, така и по време на предаване, с възможност за избор на алгоритъм за криптиране, включително AES 256-bit, и опция за използване на облачно криптиране в публичен облак без необходимост от допълнителни инструменти (SW/HW).
REQ.21	Софтуерното криптиране на предложеното решение трябва да бъде външно валидирано като FIPS 140-3 сертифицирано.
REQ.22	Предложеното решение трябва да поддържа сигурна репликация на данни в изолирана среда с възможности за "въздушна пропаст" (air gap), оркестрирана чрез рамка за работни процеси, която изпълнява и контролира скриптове, API заявки или командни операции.
REQ.23	Предложеното решение трябва да включва вградена висока наличност и възстановяване след бедствия на сървъра за управление на архивите, за да гарантира, че е готов за възстановяване след бедствия и има способността бързо да превключва към резервен сървър в случай на бедствие.
REQ.24	Предложеното решение трябва да поддържа QoS (качество на услугата) настройки и регулиране (throttling) на мрежовия трафик на клиентите.

Минимални технически изисквания	
REQ.25	Предложеното решение трябва да поддържа архивиране на бази данни на Oracle – файлове с данни, tablespaces, контролни файлове, лог файлове и сървърни параметри – в онлайн и офлайн режим, с или без RMAN каталог, архивиране и възстановяване на ниво блок, както и автоматично архивиране на лог файлове при определени условия, напр. когато местоназначението за архивиране на лог файловете достигне определен капацитет.
REQ.26	Предложеното решение трябва да поддържа онлайн архивиране на Oracle за Windows, Linux (RHEL, OEL, SuSE и др.) и Unix платформи като HP-UX, Solaris, AIX и др.
REQ.27	Предложеното решение трябва да поддържа създаването на клонирани или standby копия на Oracle бази данни от продукционна среда, включително инкрементална репликация и поддържане на синхронизирани копия за целите на възстановяване при бедствия, както и възстановяване на Oracle бази данни между различни машини и платформи.
REQ.28	Предложеното решение трябва да поддържа автоматично откриване на SQL инстанции във физически и виртуални машини, конфигурации на MS SQL Always On с единна точка за архивиране и възстановяване, възстановяване към определен момент във времето, възстановяване на индивидуални таблици и блоково архивиране на SQL бази данни.
REQ.29	Предложеното решение трябва да поддържа базирано на моментни снимки (snapshot) архивиране и възстановяване на SQL бази данни, включително за инстанции с Always On, както и възстановяване на физически горещ резервен сървър (hot standby) за намаляване времената за възстановяване на продукционни SQL инстанции.
REQ.30	Предложеното решение трябва да осигурява вградена възможност за архивиране в облака – съхраняване на основни или вторични копия, включително записване на дедуплицирани и компресирани данни в облачни архивни нива – без използване на шлюзове, устройства, допълнителен софтуер или скриптове на трети страни.
REQ.31	Предложеното решение трябва да поддържа динамично разпределение на ресурсите в облака, включително "cloud burst" чрез автоматично мащабиране нагоре или надолу при необходимост, и управление на енергийната ефективност на облачните ресурси.
REQ.32	Предложеното решение трябва да поддържа облачни бази данни (DBaaS) в AWS, Azure и други платформи, включително защита на бази данни чрез два метода: защита чрез моментни снимки, използвайки вградени RDS моментни снимки и репликация на моментни снимки между региони и акаунти, както и защита, репликация и достъп до криптирана RDS инстанция в нова дестинация без необходимост от декриптиране и повторно криптиране на данните.
REQ.33	Предложеното решение трябва да осигурява вградено архивиране и възстановяване на контейнери за Docker, Kubernetes и OpenShift, защитавайки приложения, постоянни обеми (PV), ресурси (CRDs) и всички компоненти на средата, независимо дали работят локално, в облака или в управлявани Kubernetes PaaS услуги (като GKE, EKS, AKS), с поддръжка на CNCF-сертифицирани Kubernetes дистрибуции и Container Storage Interface (CSI) драйвери. Управлението на защитата и възстановяването на Kubernetes приложения трябва да отговаря на изискванията за единен интерфейс по REQ.6.
REQ.34	Предложеното решение трябва да може да архивира, възстановява и мигрира Kubernetes приложения със запазено (stateful) състояние и данни – pod, deployment, StatefulSet или друг workload, заедно с постоянните им дискове (PV) и

Минимални технически изисквания	
	заявки за постоянни дискове (PVC) – като автоматично ги открива и защитава чрез етикети (labels), селектори или пространства от имена (namespaces).
REQ.35	Предложеното решение трябва да може да: a) възстанови цяло Kubernetes приложение към предишна точка във времето, включително автоматично разгръщане на ново приложение или в нов Kubernetes клъстер; b) възстанови подприложение (sub-application) от композитно (custom resource) приложение; c) възстанови индивидуален обем с данни от приложение, за да бъде прикачен към ново приложение; d) възстановява или изтегля файлове и папки от дискови обеми с данни, както и YAML манифести на приложения.
REQ.36	Предложеното решение трябва да осигурява цялостна защита на виртуални машини без използване на агенти – пълно, инкрементално и синтетично пълно архивиране, с пълно възстановяване на виртуални машини, дискове и файлове – като архивира приложенията, запазвайки тяхната цялост, без инсталиране на агенти за приложения, автоматично открива и класифицира виртуалните машини в политики за архивиране и разпределя динамично виртуалните машини между наличните прокси сървъри както в началото на архивната задача, така и по време на нейното изпълнение.
REQ.37	Предложеното решение трябва да поддържа функция за live mount – стартиране на временна виртуална машина директно от резервно копие – и възстановяване на виртуални машини в реално време (live VM recovery), без да се чака пълно възстановяване.
REQ.38	Предложеното решение трябва да може да репликира виртуални машини в топъл (warm) резервен център за възстановяване при бедствия по график и да поддържа операции за възстановяване при бедствия както при поискване, така и по график, със следните сценарии: Репликация от основен към вторичен сайт DR оркестрация между основния и вторичния сайт Групи за автоматизирано превключване при аварии на група виртуални машини Виртуални лаборатории, създадени като част от конфигурацията на група за аварийно превключване Валидация на приложения в сигурна изолирана мрежова среда преди възстановяването им в продукционна среда
REQ.39	Предложеното решение трябва да поддържа инкрементална репликация от резервно копие на виртуална машина или база данни към синхронизирано копие на източника, включително репликиране на виртуални машини от локална среда към облачна инфраструктура.
REQ.40	Предложеното решение трябва да поддържа архивиране на хранилища за обектно съхранение, съдържащи данни, създадени от други приложения на трети страни, било то в облака, към алтернативен доставчик или обратно към локални среди.
REQ.41	Поддръжка от производителя за срок от минимум 3 (три) години.

Предлаганото решение трябва да съответства или да надвишава, в техническо отношение, посочените минимални изисквания.

2.2 Минимални изисквания за дейност 2 – „Осигуряване на web application firewall за срок от 5 години“

Целта на дейност 2 е осигуряване на защитни стени на ниво уеб приложение, със следните минимални изисквания:

Минимални технически изисквания	
REQ. 1.	Предложеното решение трябва да включва 2 броя лицензи за софтуер за мониториране и защита на мрежови приложения (WAF) за капацитет от минимум 1Gbps с валидност и включена поддръжка минимум за срок от 60 месеца.
REQ. 2.	Решението да позволява използването на минимално 8 виртуални устройства, като част от лицензa, които да могат да се поставят минимално на следните хипервайзори: VMware ESX и ESXi, KVM, Hyper-V.
REQ. 3.	Решението трябва да предоставя гъвкава пропускателна способност, използвайки vSwitch функцията на даден хипервайзор.
REQ. 4.	Решението трябва да поддържа възможности за ускорение на уеб приложения, минимално кеширане, компресия и модифициране на хедър (header).
REQ. 5.	Решението трябва да поддържа функция за мониториране на състоянието (Health Monitoring) на уеб трафика. Минимално да се поддържат следните протоколи за мониториране: ICMP, TCP и UDP, HTTP и HTPPS (като решението да може да маркира недостъпни в даден момент точки), LDAP и LDAPS, FTP, SNMP, DNS, IMAP4, NNTP, на ниво физически портове, POP3, RADIUS, RTSP, SMTP, чрез SSL Hello, на ниво UDP порт, SIP UDP/SIP TCP, OCSP.
REQ. 6.	Решението трябва да поддържа функция за бърза TCP проверка на състоянието (Health Check) на уеб трафика.
REQ. 7.	Решението трябва да поддържа проверки на състоянието на уеб трафика, базирани на L2 (ARP), L3 (PING) и L4 (TCP/UDP проверки на портове).
REQ. 8.	Решението трябва да предоставя предефинирани L7 проверки на състоянието на ниво приложение (HTTP, HTTPS, LDAP, SMTP и др.) и персонализиране на проверки за всякакви бинарни и текстово базирани протоколи.
REQ. 9.	Решението трябва да може да засича статуса на сървъри, на база събрани и обработени данни от проверки на състоянието.
REQ. 10.	Решението трябва да може да засича статуса на сървъри, на база зададени логически изрази при сравнение на данни от множество проверки на състоянието.
REQ. 11.	Решението трябва да може да засича претоварване на сървъри, чрез проверки на състоянието .
REQ. 12.	Решението трябва да позволява да се определя интервала на събиране на данни за мониториране.
REQ. 13.	Решението трябва да позволява да се определя максималното допустимо време без отговор при събиране на данни за мониториране (timeout interval).
REQ. 14.	Решението трябва да поддържа проверяване на състоянието на сървъри чрез външни скриптове, минимално Python-базирани.
REQ. 15.	Решението трябва да може да балансира трафика от уеб приложения на слоеве 4 до 7 от OSI модела, минимално на база използван протокол (TCP, UDP), IP адреси на източник/дестинация, съдържание на приложения (минимално URL адреси, бисквитки, хедъри, текст, HTML тагове, XML тагове, DNS домейн, тип заявка).

REQ. 16.	Решението трябва да може да балансира трафика минимално на база най-бърза връзка, количество входящ и изходящ трафик, брой едновременно свързани потребители, тежест, точки с най-малко свързвания.
REQ. 17.	Решението трябва да може да показва страница с информация за грешка при недостъпност на даден ресурс/application сървър. Страницата с информацията за грешката трябва да подлежи на конфигурация, включително относно графичните елементи в нея.
REQ. 18.	Решението трябва да разполага с функция за осигуряване на постоянна свързаност на мрежови сесии, минимално на база IP адрес на източник, бисквитки, ID на SSL сесия, IP хеширане.
REQ. 19.	Решението трябва да поддържа следните протоколи за рутиране, минимално: OSPF, OSPFv3, RIP 1 /RIP 2 и BGP-4.
REQ. 20.	Решението трябва да поддържа минимално следните функционалности: SSL offload, възможност да управлява SSL трафика на клиента, като прекъсва входящи SSL връзки и да изпраща заявки към сървъра в чист текст.
REQ. 21.	Решението трябва да поддържа възможност за пропускане на IP адреси на клиента до крайния сървър през SSL (възможност за работа на решението като прозрачно прокси).
REQ. 22.	Решението трябва да поддържа SHA2 (Secure Hashing Algorithm).
REQ. 23.	Решението трябва да поддържа управление на сървърни сертификати на ниво виртуална услуга (Virtual Service Level).
REQ. 24.	Решението трябва да поддържа използването на TLS версии 1.2 и 1.3.
REQ. 25.	Решението трябва да поддържа функции за TCP и HTTP мултиплексиране.
REQ. 26.	Решението трябва да поддържа HTTP компресиране.
REQ. 27.	Решението трябва да позволява селективно HTTP компресиране, за да избегне познати проблеми с компресирането в често използвани браузъри.
REQ. 28.	Решението трябва да поддържа функция за уеб кеширане в съответствие с RFC 2616 на HTTP 1.1.
REQ. 29.	Решението трябва да поддържа функция за оптимизиране на кешираните данни в клиентски браузър минимално чрез пренаписване на атрибути или чрез промяна на хедърите на обекти.
REQ. 30.	Решението трябва да позволява автоматично девалидиране на кеширани данни, базирано на дадено взаимодействие на потребителите с дадено уеб приложение.
REQ. 31.	Решението трябва да поддържа TCP оптимизиране.
REQ. 32.	Решението трябва да поддържа функция за ускоряване на доставянето на услуги в клетъчни и безжични среди.
REQ. 33.	Решението трябва да може да използва услуги за сигурност от облака на производителя, дори когато е разположено локално, минимално за WAF защита,
REQ. 34.	Решението трябва да поддържа защита от ботове, включително поддръжка на използване на Captcha механизъм.
REQ. 35.	Решението трябва да поддържа информация за активни хакери, под формата на списък, който се актуализира в реално време, позволявайки на решението да блокира хакери, преди те да предприемат злонамерени действия.
REQ. 36.	Решението трябва да поддържа функция за филтриране на мрежови пакети за контрол на достъпа.
REQ. 37.	Решението трябва да разполага с конзола за централизирано управление на всички негови компоненти и устройства. Конзолата да може да е достъпна през уеб-браузър.
REQ. 38.	Решението трябва да поддържа използването на SNMP версии 1,2 и 3.
REQ. 39.	Решението трябва да разполага с добре документиран API интерфейс за интегриране с персонализирани приложения.

REQ. 40.	Решението трябва да позволява изпращането на логове към сървър чрез Syslog. Минимално да се поддържат следните формати: BSD syslog-RFC3164 и IETF syslog-RFC5424.
REQ. 41.	Решението трябва да поддържа ролево-базирано управление. Минимално да могат да се лимитират правата на потребителите на решението да управляват: няколко устройства, конфигурацията на едно устройство, специфичен обект и неговата конфигурация или конкретен сървър.
REQ. 42.	Решението трябва да поддържа AAA модел на автентикация на отдалечени потребители, да се поддържат минимално RADIUS, TACACS+ и LDAP.
REQ. 43.	Решението трябва да поддържа използването на резервни методи за автентикация (например използване на локален акаунт), които автоматично да се активират, ако сървърът за отдалечената автентикация е временно недостъпен.
REQ. 44.	Решението трябва да поддържа функция за мониторирането на устройствата му и техните състояния в реално време.
REQ. 45.	Решението трябва да може да съхранява две инстанции на операционната си система, с възможност за активиране/деактивиране на която и да е от тях при необходимост.
REQ. 46.	Решението трябва да поддържа инструмент за съветване при актуализации (upgrade на софтуера на решението), който автоматично да анализира конфигурацията на решението и да индикира необходимите стъпки, които трябва да се предприемат, преди актуализацията да се извърши.
REQ. 47.	Решението трябва да предоставя вградени инструменти за събиране на мрежови пакети (подобно на TCPdump).
REQ. 48.	Решението трябва да може да криптира всички пароли в конфигурационните му файлове.
REQ. 49.	Решението трябва да може да предоставя отчет/анализ на състоянието на уеб приложенията и статистика за всички управлявани устройства.
REQ. 50.	Решението трябва да може да предоставя анализи за производителността на уеб приложенията и управляваните устройства, като трябва да може да съхранява информацията в исторически план.
REQ. 51.	Решението трябва да може да предоставя информация за всяко приложение за внесено забавяне (latency) на ниво мрежа и на ниво приложение.
REQ. 52.	Решението трябва да позволява извличането на отчети в различни формати, минимално HTML и PDF.
REQ. 53.	Решението трябва да предоставя изглед (dashboard) с информация за транзакциите на всяко от уеб приложенията, минимално информация за GEO локация и използван браузър.
REQ. 54.	Решението трябва да може да идентифицира минимално аномалии в трафика, причини за проблеми с SSL и HTTP сесии, възникване на бавни отговори и причината за забавянето, както и да може да различава нормални транзакции от такива, свързани с атаки.
REQ. 55.	Решението трябва да поддържа „Топ 5“ класации за уеб приложения базирани на информацията от транзакции с тях. Минимално топ 5 имена на хостове, използвани методи, път за свързване, използвани браузъри, IP адреси на източници.
REQ. 56.	Решението трябва да поддържа делегирането на поддомейн, който да служи за обработването на всички DNS заявки и multi-homed услуги.
REQ. 57.	Решението трябва да поддържа функция за групиране на няколко DNS сървъра.
REQ. 58.	Решението трябва да се предоставя чрез единен глобален лиценз, който да предоставя всички необходими функционалности и услуги.

REQ. 59.	Решението трябва да предоставя опция за управление чрез глобален лицензионен сървър при необходимост, разположен в облака на производителя, без да се налага инсталирането на локален лицензионен сървър.
Гаранция и поддръжка:	
REQ. 60.	Период на поддръжка: минимум 60 месеца
REQ. 61.	Тип поддръжка: 24x7x365
REQ. 62.	Възможност за обновление на софтуера в периода на поддръжката до последна актуална версия на производителя.

Предлаганите устройства трябва да съответстват или да надвишават, в техническо отношение, посочените минимални изисквания.

3. МЯСТО НА ДОСТАВКА И ПОДДРЪЖКА

3.1. Мястото на доставка е сградата на НЗОК – гр. София, ул. „Кричим" № 1

3.2. Услугите по поддръжката се предоставят отдалечено, при необходимост от оказване на съдействие на място, в сградата на НЗОК – гр. София, ул. „Кричим" №1

4. ДОПЪЛНИТЕЛНИ ИЗИСКВАНИЯ

- Доставените продукти следва да са нови, неупотребявани, нерециклирани към датата на доставка и различни от доставените по Договор № BG16RFPR002-2.018-0001-C01/06.11.2025 г. „Повишаване на националните способности за координация и реагиране при инциденти, свързани с киберсигурността".
- Изпълнителят следва да осигури изпълнението от лице надлежно оторизирано от производителя или официален негов представител за правото на разпространение/доставка на предлаганите продукти на територията на Република България.
- Заявки за обслужване (тикети) за доставения хардуер се подават чрез осигурена от Изпълнителя онлайн система за управление на заявки (СУЗ). Всички заявки, получени чрез електронна поща или телефон следва да бъдат регистрирани в СУЗ.

5. ИЗИСКВАНИЯ КЪМ МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ[2]

5.1 Изпълнителят следва да осигури прилагането на изискванията на Закона за електронното управление, Закона за защита на личните данни, Закона за киберсигурност и подзаконовите нормативни актове към тях.

5.2 Във връзка с мрежовата и информационната сигурност на Бенефициера (НЗОК) и в съответствие с чл. 10 от Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС), Изпълнителят:

(а) Гарантира, че лицата, ангажирани от Изпълнителя с изпълнението на Услугата (в т.ч. подизпълнители, когато е приложимо) и които ще имат достъп до информация и активи, при взаимодействието им със служители на Бенефициера (НЗОК), ще спазват изискванията за сигурността на информацията съгласно Закона за киберсигурност и НМИМИС.

[2] Изискванията към мрежовата и информационната сигурност са приложими, в случай, че по време на изпълнение на заявката Изпълнителят (подизпълнителите, когато е приложимо) имат достъп до информация и активи на Бенефициера (НЗОК), които са предмет на защита съгласно приложимото законодателство в областта.

(б) При предоставяне на Услугата спазва правилата за сигурността на информацията на Бенефициера (НЗОК). За целта, непосредствено преди началото на изпълнение, ангажираните от Изпълнителя за предоставяне на Услугата лица (в т.ч. и подизпълнителите, когато е приложимо), които ще имат достъп до информация и активи на Бенефициера (НЗОК), подписват декларации по образец на Изпълнителя за опазване на информацията, които се предават на Бенефициера (НЗОК). При промяна на лицата в хода на изпълнението съответните подписани декларации се предават, в срок до два работни дни от промяната.

(в) определя компетентното лице, отговорно за мрежовата и информационна сигурност, което осъществява взаимодействие с компетентно лице от страна на Бенефициера (НЗОК) при възникване на инцидент по МИС.

(г) осигурява адекватни и комплексни мерки за защита за мрежова и информационна сигурност, основани на извършения анализ и оценка на риска, с цел да се гарантира необходимото ниво на сигурност. Имплементираните смекчаващи механизми трябва да са пропорционални на рисковете, в частност на щетите, които те биха могли да нанесат.

5.3 Изпълнителят се задължава да не разпространява информация, станала му известна при и по повод изпълнението на Услугата на трети страни без изричното писмено съгласие на Бенефициера (НЗОК).

5.4 Лицата, отговорни за мрежовата и информационната сигурност и параметрите на нивото на обслужване при изпълнение на Заявката („лица по чл. 10, ал. 2 от НМИМИС“) имат следните права и задължения:

(а) При изпълнението на задълженията си, осъществяват комуникация с лицата, които ще имат достъп до системите на съответната администрация;

(б) Лицето по чл. 10, ал. 2 от НМИМИС от страна на Изпълнителя отговаря за прилагането на адекватни мерки за мрежова и информационна сигурност от страна на Изпълнителя (и на подизпълнителите, когато е приложимо);

(в) При получена информация, лица по чл. 10, ал. 2 от НМИМИС осъществяват незабавна комуникация по телефон и/или имейл и предприемат действия за извършване на анализ на: причините за влошаване на качеството по отношение на времената за реакция и за възстановяването на работата; условията, при които инцидентът може да бъде затворен; рискът за постигане на целите на мрежовата и информационната сигурност на Бенефициера (НЗОК);

(г) При констатирано неспазване на изискванията за сигурност на информацията или неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за мрежовата и информационната сигурност за Бенефициера (НЗОК), лицата по чл. 10, ал. 2 от НМИМИС съвместно с лицата, които ще имат достъп до системите на съответната администрация от страна на Бенефициера (НЗОК) и на Изпълнителя извършват анализ и набелязват мерки за отстраняване на допуснатата нередност в определен срок.