Приложение № 2
към рамков договор № 1005-40-42 от 08.06.2026 г.

ЗАЯВКА по Рамков договор № 1005-40-42 от 08.06.2026 г. **(вх. № ПО-16-2118/08.06.2026г. на ИО АД)**	☒
ЗАЯВКА по Рамков договор № …….от ……г. **(актуализирана)**	☐ [1]

Позиция от ПГ-2026 г.:	*№ по ред от ПГ*	*Ред 26 и ред 27*
Описание на проект съгласно ПГ:	*Доставка на устройства за защита на Web приложения (WAF) и на защитни стени от ново поколение за нуждите на Национален осигурителен институт (НОИ)*	
CPV код	*72000000-5*	
Рег. номер на писмо от МИДТ за утвърждаване на проекта /становище по проекта	*МИДТ-33-00-69/16.07.2026*	
Изискване за достъп до класифицирана информация ДА/НЕ	*НЕ*	
Стойност: (*стойността следва да съответства на заложената в План-графика***) евро без ДДС**, *в т.ч. разбивка на стойността за проекти на части/ с акредитив/ авансово*	*Ред 26 от ПГ 2026 – 227 680,00 евро без ДДС* *Ред 27 от ПГ 2026 – 246 720,00 евро без ДДС*	
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*	*Еднократно, след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ доставката на защитни стени и издадена фактура.*	
Плащане с акредитив или авансово ДА/НЕ	*НЕ*	
Документи за плащане с акредитив или авансово	*НЕ*	
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 поддръжката - 36 месеца от осигуряване.*	
Гаранционен срок: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*Съгласно техническите параметри*	

[1] Отбелязва се в случай че заявката е актуализирана

Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*	*Еднократно, с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ доставката на защитни стени.*
Приложения: (*напр: технически параметри, образци на отчетни документи*)	*Технически параметри (ТП)*
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	*Подпис:*

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

страна на БЕНЕФИЦИЕРА:		
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

„Доставка на устройства за защита на Web приложения (WAF) и защитни стени от ново поколение за нуждите на Национален осигурителен институт (НОИ)”

Гр.София, 2026г

1. ПРЕДМЕТ

В предмета на заявката се включва доставка на устройства за защита на Web приложения (WAF) и защитни стени от ново поколение, 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“, за нуждите на Национален осигурителен институт (НОИ).

2. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО

Минималните изискванията на Бенефициера относно обхвата и изпълнението на дейностите по доставка на устройства за защита на Web приложения (WAF) и защитни стени от ново поколение за нуждите на Национален осигурителен институт (НОИ), са както следва:

2.1 **Минимални изисквания по ред 26 – „Доставка на устройства за защита на ниво web приложения WAF“**

3. Минимални изисквания	
	Количество – 2 броя
REQ.1	Да разполага с минимум два резервирани AC захранващи блока
REQ.2	Да разполага с минимум 2 слота QSFP28/QSFP+ поддържащи 40G, 100G интерфейси
REQ.3	Да разполага с минимум 8 слота SFP28/SFP+/SFP поддържащи 25G, 10G интерфейси
REQ.4	Всяко устройство да бъде оборудвано с не по-малко от 2 броя SFP+ 10GBASE-SR интерфейса с инсталирани минимум 2 броя SFP+ 10GBASE-SR трансивъри, от производителя на предложеното оборудване или сертифицирани от него.
REQ.5	Да разполага с минимум 1 брой порт за управление 1000BASE-T
REQ.6	Да разполага с минимум 1 брой USB 3.0
REQ.7	Да разполага с минимум 1 брой сериен конзолен порт
REQ.8	Да разполага с минимум един SSD диск с размер не по-малък от 950GB
REQ.9	Да има следната минимална производителност за управление на трафика: ● 2,400,000 заявки в секунда L7 ● 980,000 конекции в секунда L4 ● 17,800,000 HTTP заявки в секунда L4 ● 75,000,000 едновременни конекции L4 ● 90Gbps пропускателна способност L4 ● 58Gbps пропускателна способност L7
REQ.10	Да включва хардуерен offload на SSL/TLS с минимум 35Gbps bulk encryption и минимум 59,000 транзакции в секунда при използване на 2K SSL ключове

3. Минимални изисквания	
REQ.11	Устройството да предлага възможност за бъдещо разширение до 44Gbps bulk encryption и 79000 транзакции в секунда при използване на 2K SSL ключове
REQ.12	Да разполага с минимум 16 ядрен процесор
REQ.13	Да е с инсталирана памет не по-малко от 128GB
REQ.14	Да поддържа софтуерна компресия с капацитет от минимум 33 Gbps и да позволява бъдещо надграждане с поддръжка на хардуерна компресия с капацитет минимум 38 Gbps
REQ.15	Да поддържа конфигуриране и управление през API интерфейс
REQ.16	Да включва минимум следните методи за балансиране на трафика: ● Round Robin; ● Least Sessions; ● Least Connections; ● Weighted Least Connection; ● Ratio.
REQ.17	Да включва функционалност за наблюдение на състоянието на сървърите към услугата, която балансира на база минимум следните протоколи и системи: TCP, UDP, FTP, Gateway, HTTP, HTTPS, ICMP, за да разпределя заявките само до наличните сървъри
REQ.18	Да включва функционалност (Persistence) за изпращане на заявките от един потребител към един и същи сървър в мрежата на база на Source IP, Destination IP, Cookies, Host
REQ.19	Устройството да има Full Proxy архитектура
REQ.20	Устройството да има функционалност за разделяне на минимум 8 виртуални устройства/контекста с възможност за бъдещо надграждане на поддържаните виртуални устройства/контексти до минимум 18 броя
REQ.21	Да включва функционалност за защита на Web приложения (Web Application Firewall, WAF) със следните функционалности: ● Защита от атаки насочени към приложния слой - Layer 7 Attack Protections; ● Защита и предотвратяване на OWASP Top 10 атаки с визуално представяне на информация за нивото на съответствие на приложените политики за сигурност спрямо отделните атаки съгласно препоръките на OWASP; ● Откриване и смекчаване на L7 DoS/DDoS атаки; ● Автоматично създаване на сигнатури, базирани на поведението на трафика и състоянието/натоварването на защитените сървъри за смекчаване на L7 DoS/DDoS атаки – L7 Behavioral DoS protection; ● Създаване на политики за защита на приложенията, чрез импорт на OpenAPI файлове; ● Поддръжка на JSON schema валидация; ● Защита и смекчаване на Brute force атаки; ● Защита и смекчаване на Heavy URLs атаки; ● Защита от Web Scraping ● Device fingerprinting; ● Разпознаване и защита от злонамерени ботове; ● Блокиране на заявки на база геолокация; ● Терминиране на SSL с повторно криптиране; ● Защита на полета с чувствителна информация в браузера на клиента

3. Минимални изисквания	
	(потребителски имена, пароли и др.) без да е необходима инсталация на софтуер или агенти на клиентската машина. ● Защита на приложно-програмни интерфейси (Application Programming Interface, API) ● DAST (Dynamic Application Security Testing) интеграция.
REQ.22	Да позволява бъдещо надграждане с функционалност за L3/L4 защитна стена, разпознаване на аномалии на ниво протокол и механизми за предотвратяване на DDoS атаки на ниво L3/L4.
REQ.23	Да позволява бъдещо надграждане с функционалност за реализиране на SSL VPN, регистрация на много услуги с една автентикация Single sign-on (SSO) с поддръжка на стандарт SAML 2.0.
REQ.24	Да позволява бъдещо надграждане с функционалност за DNS сървър, DNS SEC, DNS защитна стена с механизми за предотвратяване на DDoS атаки на ниво DNS, балансиране на услуги на ниво DNS между географски отдалечени Active/Active центрове за данни.
REQ.25	Да включва достъп до SaaS платформа, позволяваща следните функционалности: · Услуга за динамично тестване на сигурността на приложенията (DAST) - извършва автоматизирано сканиране на публично достъпни уеб приложения за идентифициране на уязвимости (по стандарта OWASP Top 10). · Cloud-Native услуга за глобално балансиране на натоварването (GSLB) - трябва да оперира независимо от хардуера в локалния център за данни, осигурявайки DNS-базирано управление на трафика между множество центрове за данни и облачни доставчици. Услугата трябва да включва вградена DDoS защита за DNS инфраструктурата и да позволява мигновено пренасочване (failover) без необходимост от инсталиране на физически DNS устройства във всяка локация. · Модул за защита на API и управление на бот трафик (WAAP) - системата трябва да използва клиентска телеметрия и поведенчески анализ (Behavioral Analysis) в реално време, за да идентифицира и блокира усъвършенствани автоматизирани заплахи (като 'credential stuffing' и 'scraper' ботове), преди те да достигнат до локалната инфраструктура. Допълнително, модулът трябва да осигурява автоматично откриване на API крайни точки (API Discovery) за визуализиране на 'Shadow APIs' и да позволява налагане на позитивен модел на сигурност чрез директен импорт на OpenAPI/Swagger спецификации, блокирайки заявки, които не отговарят на дефинираната схема.
REQ.26	Да включва достъп до актуална база с репутация на IP адреси с цел управление/ограничаване на достъпа до услугите от IP адреси с лоша репутация;
REQ.27	Да включва права за ползване или абонамент за достъп до актуална база от данни със сигнатури за защита от координирани атаки и заплахи, както и актуална база данни със сигнатури за разпознаване на злонамерени ботове.
REQ.28	Да има уеб базиран потребителски интерфейс (UI) достъпен през HTTPS
REQ.29	Да има CLI базиран потребителски достъп през конзола и SSH
REQ.30	Да бъде окомплектовано с необходимите елементи за монтаж в 19” комуникационен шкаф
Гаранция	

3. Минимални изисквания	
REQ.31	Гаранционно обслужване от минимум 36 (тридесет и шест) месеца в режим 8x5xNBD
REQ.32	Възможност за получаване на нови версии на софтуера за срок от минимум 36 (тридесет и шест) месеца.
REQ.33	Устройството е окомплектовано със съответните лицензи и права за използване според условията на производителя.

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

2.2 Минимални изисквания по ред 27 – „Доставка на защитни стени от ново поколение“

Обща информация	
REQ.1.	Количество – 2 броя.
Спецификация – минимални изисквания	
REQ.2.	Минимална пропускателна способност с активирана функция за идентификация на приложенията - 18 Gbps.
REQ.3.	Минимална пропускателна способност с активирани всички функционалности за защита: IPS/ AntiVirus/AntiMalware/URL/Firewall/Application Control – 10 Gbps.
REQ.4.	Минимална производителност за IPsec VPN – 9 Gbps.
REQ.5.	Минимален брой сесии - 2 200 000.
REQ.6.	Минимален брой нови сесии в секунда - 220 000.
REQ.7.	Разпознати и поддържани приложения – минимум 3 650 броя.
REQ.8.	Минимален брой мрежови интерфейси: • Да разполага с 12x1/2.5/5/10G Base-T ports; • Да разполага с 10x1/10G SFP/SFP+ интерфейса; • Да има възможност за допълнителни минимум 4x25G SFP28.
REQ.9.	Режими на работа на интерфейсите: • L2; • L3; • Tap; • Transparent; • едновременно/микс да се използват върху едно устройство.
REQ.10.	Машрутизиращи протоколи: • OSPFv2/v3; • BGP with graceful restart; • RIP; • Static routing; • Policy-based forwarding; • Point-to-Point Protocol over Ethernet (PPPoE);

Обща информация	
	• Bidirectional Forwarding Detection (BFD).
REQ.11.	Минимални изисквания към IPSec имплементация: • Key exchange: manual key, IKEv1 and IKEv2 (pre-shared key, certificate authentication); • Encryption: 3DES, AES (128-bit, 192-bit, 256-bit) Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512.
REQ.12.	Минимален брой конкурентни SSL VPN потребителя, включени в системата (постоянни лицензи) - 1000 SSL VPN потребителя.
REQ.13.	Минимален брой IPSec Site-to-Site VPN - 2000 отдалечени точки.
REQ.14.	Устройството да поддържа виртуални таблици за маршрутизация минимум 11 броя.
REQ.15.	Устройството да има възможност да поддържа виртуализация (виртуални контексти) – 11 броя.
REQ.16.	Всички конфигурации за интерфейсните модули на защитната стена трябва да поддържат IPv6, както и всички контролни функции на системата трябва да се налични и за IPv6.
REQ.17.	Системата следва да декриптира и инспектира SSL като поддържа: TLS v1.1, TLS v1.2, TLS v1.3.
REQ.18.	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.
REQ.19.	Режим на надеждност: • Active-Passive; • Active/Active; Клъстер до 6 устройства разпределени в отдалечени центрове за данни.
REQ.20.	Минимален брой делегирани интерфейси за управление (в допълнение на мрежовите интерфейси): • 1 x 10/100/1000 out-of-band management port; • 2 x 100/1000Mbps, 1 x 10Gbps SFP+ интерфейси за отказоустойчивост; • 1 x RJ-45 конзолен порт.
REQ.21.	Предназначена за вграждане в 19" шкаф с максимален размер 1U.
REQ.22.	Резервирано, 100-240VAC (50-60Hz).
Функционални изисквания към системата	
REQ.23.	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.
REQ.24.	Системата да анализира съдържанието за наличие на зловреден код като включва минимум AntiVirus, AntiSpyware, IPS.
REQ.25.	Системата да прави анализ на непознати заплахи (Zero Day зловреден код) в защитена среда като създава и дистрибутира сигнатури в реално време.

Обща информация	
REQ.26.	Системата за анализ на Zero Day зловреден код трябва да използва минимум следните методи за анализ: Static Analysis, Machine Learning, Dynamic Analysis, Bare metal analysis.
REQ.27.	Предлаганата защитна стена трябва да може да изпраща минимум 2000 файла на час към системата за анализ на Zero Day.
REQ.28.	Системата да анализира PE и PowerShell скриптове в защитната стена и предоставя защита в реално време.
REQ.29.	Системата следва да инспектира за заплахи HTTPS протокола чрез декриптиране.
REQ.30.	Системата следва да инспектира за заплахи HTTP 1.1 и HTTP 2.0 протоколи.
REQ.31.	NGFW възможностите и прилежащите бази данни като Antivirus, Sandboxing трябва да използват сигнатури и съдържание на производителя на защитната стена – Не се приема OEM или интеграция с трети страни.
REQ.32.	Управлението на устройството трябва да се реализира чрез физически отделени процесор и памет отделени от ресурсите използвани за управление на трафика.
REQ.33.	Решението да използва вътрешните ресурси на защитната стена, за да анализира и открива зловреден JavaScript с цел кражба на корпоративни потребителски имена и пароли чрез Phishing.
REQ.34.	Наличие на DLP (Data Loss Prevention) функционалност, за ограничаване на движението на конфиденциални файлове към и извън организацията.
REQ.35.	Решението да притежава възможност да ограничава достъпа на потребителите до Web сървъри, които не поддържа минимални изисквания за валиден публичен сертификат и съответно високо ниво на сигурност (TLSv 1.1, TLSv1.2, TLSv1.3).
REQ.36.	Препращане на подозрителните DNS заявки към устройството с цел ограничаване на достъпа и регистриране на заразени машини в мрежата.
REQ.37.	Предложеното решение трябва да може да изгражда отдалечен VPN достъп чрез агент инсталиран на крайно клиентската машина.
REQ.38.	Агента за VPN достъп трябва да поддържа (да може да бъде инсталиран) минимум следните операционни системи: Windows, Linux, macOS, Android, iOS, Raspbian, Ubunto.
REQ.39.	Възможност за QoS трафика според типа приложение потребител и/или URL категория.
REQ.40.	Прозрачна идентификация на потребителите от Активната директория без изискване на крайната машина да се инсталира агент, настройки в browser или отваряне на Web Portal.
REQ.41.	Решението да може да изпраща декриптирани потоци от данни към трети страни за допълнителен анализ след което отново да криптира трафика.
REQ.42.	Да предоставя възможност за карантина на заразени устройства независимо от техните IP адреси, локация и потребител.

Обща информация	
REQ.43.	Да предоставя възможност за съставяне на политика за сигурност базирана на устройство независимо от неговия IP Address, локация и потребител.
REQ.44.	Решението да може да чете данните в X-Forwarded-For (XFF) за идентифициране на реалния източник на данни (IP Address), когато той се намира зад други мрежови устройства.
REQ.45.	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).
REQ.46.	Решението да включва функционалност позволяваща служебния достъп до публични облачни услуги като Office 365, Google, Dropbox и YouTube, и ограничаваща достъпа до лични потребителски акаунти за същите приложения.
REQ.47.	Анализът на логовете и репортинг да се извършва от самото устройство през неговия графичен интерфейс, без да е необходима инсталация на допълнителен софтуер.
REQ.48.	Решението да притежава Уеб базиран интерфейс с различни статистики на база време, приложение, категории, потребители, заплахи и други.
REQ.49.	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).
REQ.50.	Решението да може автоматично да тегли IP, Domain или URL листи от Web Server, собственост на Възложителя или външна организация с цел ограничаване / позволяване на достъпа до гореспоменатите.
REQ.51.	Решението да може автоматично да открива какви приложения работят в организацията и да предлага лист от такива, които да бъдат добавени към нови или вече съществуващи правила за сигурност.
REQ.52.	Решението да предоставя механизъм за откриване и превенция на DNS Tunneling канали за комуникация, включително възможност да следи и ограничаване достъпа до автоматично генерирани домейни (Domain generation algorithms (DGA).
REQ.53.	Системата да има възможност за надграждане с допълнителен лиценз за филтриране на уеб сайтовете по категории и ограничаване на достъпа до опасно съдържание в Интернет, включително мулти категоризация на URL съгласно тип на съдържанието и риск. Да има възможност да анализира URL и тяхното съдържание в реално време. Всяка заявка за достъп да бъде анализирана чрез Machine Learning на база на HTTP Request, включително да може да идентифицира новорегистрирани домейни и ограничава достъпа до тях.
REQ.54.	Системата да има възможност за надграждане с допълнителен лиценз инсталиран на защитната стена, чрез който да осъществява отдалечен защитен достъп от телефони и таблети (с операционни системи iOS,

Обща информация	
	Android) и инспекция (compliance check) на крайно клиентската машина, който се извършва по време на изграждането на защитена връзка.
REQ.55.	Системата да има възможност за надграждане с допълнителен лиценз, инсталиран на защитната стена, с който да открива и управлява IoT (Internet of Things) устройства като предоставя възможност за автоматично генериране на препоръчани правила за достъп и контрол.
Гаранция и поддръжка:	
REQ.56.	Хардуерна гаранция за срок от минимум 36 (тридесет и шест) месеца.
REQ.57.	Техническа поддръжка за срок от минимум 36 (тридесет и шест) месеца.
REQ.58.	Получаване на нови версии на софтуера за срок от минимум 36 (тридесет и шест) месеца.
REQ.59.	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя.

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

3. МЯСТО НА ДОСТАВКА И ГАРАНЦИОННО ОБСЛУЖВАНЕ

3.1. Мястото на доставка е сградата на Национален осигурителен институт – гр. София, бул. „Ал. Стамболийски" № 62-64.

3.2. Услугите по гаранционно обслужване и техническа поддръжка се предоставят отдалечено, при необходимост от оказване на съдействие на място, в сградата на Национален осигурителен институт – гр. София, бул. „Ал. Стамболийски" № 62-64.

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 (НОИ) 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), които ще имат достъп до информация, системи, мрежи или активи на Бенефициера (НОИ), ще спазват изискванията за сигурност съгласно Закона за киберсигурност, НМИМИС, както и вътрешните правила и политики по информационна сигурност на Бенефиц.

(б) При предоставяне на Услугата спазва правилата за сигурността на информацията на Бенефициера (НОИ). 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 (НОИ), подписват декларации по образец на Изпълнителя за опазване на информацията, които се предават на Бенефициера (НОИ). 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 (НОИ), включително при възникване, управление и докладване на инцидент по МИС.

(г) осигурява адекватни, ефективни и комплексни технически и организационни мерки за защита за мрежова и информационна сигурност, основани на извършения анализ и оценка на риска, с цел да се гарантира необходимото ниво на защита , включително по отношение на доставяните устройства за защита на Web приложения и защитни стени.

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 (НОИ).

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 изпълнение на задълженията си осъществяват координация и комуникация с лицата, които ще имат достъп до системите и инфраструктурата на съответната администрация;

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

(в) При получена информация за инцидент, 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 възникване на инцидента или влошаване на

[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 (НОИ), които са предмет на защита съгласно приложимото законодателство в областта.

качеството по отношение на времената за реакция и възстановяване на работата; условията, при които инцидентът може да бъде класифициран като разрешен июили затворен; риска за постигане на целите на мрежовата и информационната сигурност на Бенефициера (НОИ);

(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 (НОИ), лицата по чл. 10, ал. 2 от НМИМИС съвместно с лицата, които ще имат достъп до системите на съответната администрация от страна на Бенефициера (НОИ) и Изпълнителя извършват анализ и определят коригиращи и превантивни мерки за отстраняване на допуснатата нередност в определен срок.