Приложение № 2

към рамков договор № РД-02-29-19/09.07.2025 г

ЗАЯВКА по Рамков договор № РД-02-29-19/09.07.2025 г (ПО-16-2225/09.07.2025 г. на ИО АД)	☑
ЗАЯВКА по Рамков договор № РД-02-29-19/09.07.2025 г (ПО-16-2225/09.07.2025 г. на ИО АД) (актуализирана)	☐ [1]

Позиция от ПГ-2025 г.:	*№ по ред от ПГ2025*	*11.1*
Описание на дейност/проект съгласно ПГ:	*Комуникационно оборудване НИФ*	
CPV код	*32420000-3*	
Рег. номер на писмо от МЕУ за утвърждаване на проекта /становище по проекта	*Рег. № МЕУ-20018/23.12.2025 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*	*48 250,00 лв без ДДС*	
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*	*Еднократно. След подписването от страните на приемо-предавателен протокол по чл. 6 от договора удостоверяващ доставката и издадена фактура.* *В случай на невъзможност за изпълнение на дейностите до края на бюджетната година - авансово плащане през м. декември 2025 г., срещу предоставена от Изпълнителя гаранция, обезпечаваща 100% стойността на*	

[1] Отбелязва се в случай че заявката е актуализирана

	авансовото плащане с вкл. ДДС 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 на осигуряване - до 4 месеца.*	
Гаранционен срок: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*Неприложимо*	
Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*	*Еднократно. С подписването от страните на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ доставката*	
Приложения: (*напр: технически параметри, образци на отчетни документи***)**	*Техническа спецификация*	
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:		
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:		
Ръководител на проект по заявката от „Информационно обслужване“ АД		*Подпис:*
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД		*Подпис:*

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

ПРИЛОЖЕНИЕ № 1

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

ЗА:

„Комуникационно оборудване НИФ“

гр. София 2025 г.

I. ПРЕДМЕТ

В предмета на заявката се включва осигуряване на комуникационно оборудване за нуждите на Национален иновационен фонд (НИФ)

II. ОБХВАТ

Обхватът на заявката се включва следното коминкационно оборудване:

1. Защитни стени:

Обща информация	
REQ.1	Количество – 2
Минимални изисквания	
REQ.2	Минимална пропускателна способност с активирана функция за идентификация на приложенията – 2.6 Gbps
REQ.3	Минимална пропускателна способност с активирани всички функционалности за защита: IPS/ AntiVirus/AntiMalware/URL/ Firewall/ Application Control – 0.9 Gbps
REQ.4	Минимална производителност за IPsec VPN – 1.5 Gbps
REQ.5	Минимален брой сесии - 190 000
REQ.6	Минимален брой нови сесии в секунда - 37 000
REQ.7	Разпознати и поддържани приложения (минимум) - 4 200 броя
REQ.8	Минимален брой мрежови интерфейси: ● Да разполага 8 x Base-T ports
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)
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) - 900 SSL VPN потребителя,
REQ.13	Устройството да поддържа виртуални таблици за маршрутизация

REQ.14	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.15	Системата следва да декриптира и инспектира SSL като поддържа : TLS v1.1, TLS v1.2, TLS v1.3
REQ.16	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.17	Режим на надеждност: ● Active-Passive ● Active/Active
REQ.18	Минимален брой делегирани интерфейси за управление (в допълнение на мрежовите интерфейси): ● 1 x 10/100/1000 out-of-band management port ● 1 x RJ-45 конзолен порт ● 2 x USB port
REQ.19	Предназначена за вграждане в 19‘‘ шкаф с максимален размер 1U
REQ.20	Резервирано, 100-240VAC (50-60Hz)
REQ.21	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя.
Функционални изисквания към системата	
REQ.22	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.23	Системата да анализира съдържанието за наличие на зловреден код като включва минимум AntiVirus, AntiSpyware, IPS;
REQ.24	Системата да прави анализ на непознати заплахи (Zero Day зловреден код) в защитена среда като създава и дистрибутира сигнатури в реално време;
REQ.25	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.26	Системата да анализира PE и PowerShell скриптове в защитната стена и предоставя защита в реално време;
REQ.27	Системата следва да инспектира за заплахи HTTPS протокола чрез декриптиране;
REQ.28	Системата следва да инспектира за заплахи HTTP 1.1 и HTTP 2.0 протоколи;
REQ.29	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.30	Управлението на устройството трябва да се реализира че физически отделени процесор и памет отделени от ресурсите използвани за управление на трафика;
REQ.31	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.32	Наличие на DLP (Data Loss Prevention) функционалност, за ограничаване на движението на конфиденциални файлове към и извън организацията;
REQ.33	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.34	Препращане на подозрителните DNS заявки към устройството с цел ограничаване на достъпа и регистриране на заразени машини в мрежата;
REQ.35	Предложението решение трябва може да изгражда отдалечен VPN достъп чрез агент инсталиран на крайно клиентската машина;
REQ.36	Агента за VPN достъп трябва да поддържа (да може да бъде инсталиран) минимум следните операционни системи: Windows, Linux, macOS, Android, iOS, Raspbian, Ubunto
REQ.37	Възможност за QoS трафика според типа приложение потребител и/или URL категория;
REQ.38	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.39	Решението да може да изпраща декриптирани потоци от данни към трети страни
REQ.40	Да предоставя възможност за карантина на заразени устройства независимо от техните IP адреси, локация и потребител.
REQ.41	Да предоставя възможност чрез допълнителен лиценз за съставяне на политика за сигурност базирана на устройство независимо от неговия IP Address, локация и потребител.
REQ.42	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.43	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.44	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.45	Анализът на логовете и репортинг да се извършва от самото устройство с през неговия графичен интерфейс, без да необходима инсталация на допълнителен софтуер.
REQ.46	Решението да притежава Уеб базиран интерфейс с различни статистики на база време, приложение, категории, потребители, заплахи и други;
REQ.47	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.48	Решението да може автоматично да тегли IP, Domain или URL листи от Web Server собственост на организацията или външна организация с цел ограничаване / позволяване на достъпа до гореспоменатите.

REQ.49	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.50	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.51	Системата да филтрира 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.52	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, Android) и инспекция (compliance check) на крайно клиентската машина, който се извършва по време на изграждането на защитена връзка;
REQ.53	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.54	Хардуерна гаранция за срок от минимум 3 (три) години.
REQ.55	Техническа поддръжка за срок от минимум 3 (три) години.
REQ.56	Получаване на нови версии на софтуера за срок от минимум 3 (три) години.

2. ЛАН Комутатори

Обща информация	
REQ.1	Количество – 2
Минимални изисквания	
REQ.2	Монтаж - в 19“ шкаф.
REQ.3	Токозахранване – модулно, с два токозахранващи модула, AC.
REQ.4	48 порта 1GE RJ45 с поддръжка на PoE+.
REQ.5	Вграден хардуерен порт за стеково свързване с производителност 80Gbps.
REQ.6	Изграждане на стек от 8 комутатора.
REQ.7	Брой USB портове – 1.
REQ.8	Сериен конзолен порт – 1.
REQ.9	Изолиране на потребителите от един и същ VLAN.

REQ.10	Идентификация и оторизация на достъпа: 802.1x идентификация и оторизация с прилагането на динамични VLAN и ACL. MAC authentication bypass. Идентификация чрез вграден Web портал. Комбиниране на методите за идентификация на един порт – 802.1x, MAC адрес, WEB идентификация. RADIUS CoA. 802.1x идентификация на повече от едно устройство на комутаторен порт. 802.1x Multi-Domain идентификация.
REQ.11	Хардуерно реализирани листи за филтриране на трафика, на база source/destination IP адреси, source/destination MAC адреси, протоколи и Layer 4 TCP/UDP номера на портове.
REQ.12	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимален брой пакети в секунда
REQ.13	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимална скорост в секунда.
REQ.14	802.1AE с 128 битово криптиране, с MKA.
REQ.15	DHCP Snooping или еквивалентен метод.
REQ.16	DHCP опция 82.
REQ.17	Dynamic ARP inspection или еквивалентен метод.
REQ.18	IP source guard или еквивалентен метод за защита от IP spoofing в мрежи с динамично и статично присвояване на IP адресите.
REQ.19	Автоматично запаметяване на използвания от първото клиентското у-во MAC адрес и блокиране на мрежовия достъп за други устройства, които се свързват към същия порт.
REQ.20	Spanning Tree защити - BPDU Guard и Root Guard.
REQ.21	Хардуерен модул за удостоверяване автентичността на хардуера и софтуера чрез използване на криптографски методи.
REQ.22	Хардуерно IP forwarding и комутиране със следните параметри: Производителност – 175 Gbps. Forwarding – 130 Mpps. MAC адреси – 16000. IPv4 маршрути – 3000. Multicast маршрути – 1000. SVI интерфейси – 512. Пакетни буфери – 6MB.
REQ.23	DRAM - 2GB.

REQ.24	Statefull Switch Over (SSO) между комутатори в един стек за следните функции: Рутиране. STP. 802.3ad.
REQ.25	Jumbo frames - 9198 байта.
REQ.26	Spanning Tree – IEEE 802.1d, 802.1w и 802.1s.
REQ.27	Функция Private VLAN.
REQ.28	Разпознаване на мрежова връзка с еднопосочна пропускливост между два комутатора от същия вид.
REQ.29	Рутинг протоколи: RIP OSPF с 1000 маршрута. Мултикас рутиране с PIM. Рутиране на база политики. VRRP
REQ.30	IEEE 802.3ad LACP протокол.
REQ.31	IEEE 802.3ad групи с портове от различни комутатори в един стек.
REQ.32	IEEE 802.1AB (LLDP) и LLDP-MED.
REQ.33	QoS със следните функции, като минимум: HQoS. 8 изходящи пакетни опашки на всеки порт. Групиране на трафика в трафични класове на база Layer2, Layer 3 и Layer 4 трафични параметри, 802.1p и DCSP маркировка. Traffic policing. Traffic policing за входящ и изходящ трафик с възможност за задаване на CIR PIR и burst параметри. Traffic shaping. Управление на пакетните опашки чрез задаване на минимално гарантирана пропускателна способност за всеки клас от общата пропускателна способност на интерфейса. Поддръжка на две приоритетни опашки (PQ) на порт. Поддръжка на Weighted Tail Drop (WTD) или еквивалентен алгоритъм за управление на задръствания. Поддръжка на Weighted Random Early Detection (WRED) или еквивалентен алгоритъм за предотвратяване на задръствания. DSCP и 802.1p маркиране на трафика на база трафични политики.

REQ.34	Протоколи и функции за управление и наблюдение: Web GUI. CLI. DNS. TFTP. FTP. NTP. SSHv2 и SNMPv3. Експортиране на трафична информация за 16000 трафични потока чрез IPFIX, NetFlow, JFlow или еквивалентен протокол към външна система за трафичен анализ. Вграден DHCP сървър. Задаване ниво на достъп до системата за всеки администратор. Traffic policing за контролиране на трафика до контролната система на комутатора. Идентификация на администраторите чрез външни RADIUS и TACACS+ системи. Отделен Ethernet порт за out of band управление и наблюдение. API интерфейс с поддръжка на GNMI, RESTCONF и NETCONF. YANG дейта модели.
REQ.35	Комплект планки за монтаж в 19“ шкаф, стеков кабел, два захранващи кабела
Гаранция и поддръжка:	
REQ.36	Хардуерна гаранция за срок от минимум 3 (три) години.
REQ.37	Техническа поддръжка за срок от минимум 3 (три) години.
REQ.38	Получаване на нови версии на софтуера за срок от минимум 3 (три) години.
REQ.39	Лицензни абонаменти за използване на софтуерни функции за срок от минимум 3 (три) години

3. Точки за безжичен достъп

Минимални изисквания на Възложителя	
REQ. 1.	Монтаж – върху окачен таван.
REQ. 2.	Захранване – 802.3at PoE+ с консумирана мощност не по голяма от 25W.
REQ. 3.	Един IEEE 802.3bz интерфейс, който поддържа 1GE и 2.5GE.
REQ. 4.	Радио диапазони – 2.4GHz и 5GHz.
REQ. 5.	IEEE 802.11a/b/g/n/ac/ax и широчина на каналите 20, 40, 80 и 160MHz за 5GHz радио диапазон.

REQ. 6.	Data rate (2.4GHz и 5GHz комбинирано) – минимум 5Gbps.
REQ. 7.	Вградена антенна система тип omnidirectional с усилване от 4 dBi за 5 GHz.
REQ. 8.	802.11ac и 802.11ax beamforming.
REQ. 9.	MRC за 802.11n, 802.11ac и 802.11ax.
REQ. 10.	BSS Coloring.
REQ. 11.	OFDMA за приемане и предаване.
REQ. 12.	Target Wake Time.
REQ. 13.	802.11ax и 802.11ac MU-MIMO.
REQ. 14.	Пакетна агрегация A-MPDU и A-MSDU.
REQ. 15.	4x4 MU-MIMO с 4 стрийма за 802.11ac и 802.11ax.
REQ. 16.	IEEE 802.11h.
REQ. 17.	IEEE 802.11d.
REQ. 18.	WPA2 и WPA3.
REQ. 19.	802.11i, AES шифроване
REQ. 20.	802.1X.
REQ. 21.	EAP методи – TLS, TTLS, PEAP, MS-CHAPv2, GTC, SIM.
REQ. 22.	Удостоверяване на софтуерната автентичност с криптографски методи -Secure Boot или еквивалентна технология.
REQ. 23.	Управление на всички функции и радио параметри чрез централен мрежови контролер.
REQ. 24.	Вграден Bluetooth 5.0 за реализиране на beacon функции.
REQ. 25.	Сериен конзолен порт.
REQ. 26.	USB порт.
Гаранция, поддръжка и лицензи	
REQ. 27.	Хардуерна гаранция за срок от мин. 3 (три) години.
REQ. 28.	Техническа поддръжка за срок от мин. 3 (три) години.
REQ. 29.	Предоставяне на нови версии на софтуера за срок от мин. 3 (три) години.
REQ. 30.	Лицензни абонаменти за използване на софтуерни функции за срок от мин. 3 (три) години.

III. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО

- Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя или официален негов представител за право на разпространение на предлаганите продукти на територията на Република България;
- Оборудването трябва да съответства или да надвишава в техническо отношение посочените минимални изисквания в настоящите Технически параметри;
- Оборудването, предмет на доставката, трябва да бъде фабрично ново, неупотребявано, да е в актуалните продуктови листи на производителя и да не е спряно от производство;
- Хардуерните компоненти на оборудването следва да отговарят на всички стандарти в Република България относно ергономичност, пожарна безопасност, норми за безопасност и включване към електрическата мрежа;
- Хардуерът следва да бъде доставен в пълно работно състояние, в оригиналната опаковка на производителя с ненарушена цялост, окомплектовано с всички необходими интерфейсни и захранващи кабели, където се изискват, както и с необходимата техническа документация (на електронен носител или чрез линкове, от които може да бъде свалена);
- В рамките на срока на гаранционно обслужване Изпълнителят отстранява за своя сметка всички повреди и/или несъответствия на оборудването, съответно подменя дефектирали части, устройства, модули и/или компоненти с нови съгласно предписанията на производителя. В гаранционното обслужване се включва замяна на част (компонент) със скрити недостатъци с нова или на цялото устройство с ново, ако недостатъкът го прави негодно за използване по предназначението му, както и всички разходи по замяната;
- 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;
- Режимът на гаранционното обслужване на хардуера е 5 дни в седмицата (от понеделник до петък), 8 часа в рамките на работното време от 9.00 ч. до 17.30 ч.
  Времето за реакция е до следващия работен ден от уведомяването;
  Време за реакция е времето от момента на уведомяване от страна на Бенефициера за възникнал проблем до обратна реакция (обаждане или пристигане на място) от ангажирани с изпълнението лица;
- Ангажираните с изпълнението лица са длъжни да осигурят преглед на място в срок не по-късно от следващия работен ден от 9.00 ч. до 17.30 ч.;
- Лицето, ангажирано с изпълнението, следва да отстрани настъпилата повреда и/или несъответствие и възстановяване на пълната работоспособност на оборудването.

Отстраняването на настъпила повреда и/или несъответствието се осъществява по местонахождението на оборудването;

- За всяка извършена дейност, свързана с гаранционното обслужване, се изготвя и предоставя протокол за извършена дейност по гаранционно обслужване, който съдържа описание на извършеното, включително вид и количество. Протоколът се подписва от ангажирано от Изпълнителя лице и оторизираното лице по място на инсталация;
- В случай, че повредата и/ или несъответствието прави устройството негодно за използване по предназначението му, ангажираното с изпълнението лице е длъжно да го замени с ново, с параметри, гарантиращи същата или по-добра функционалност и производителност.

IV. МЯСТО НА ДОСТАВКА

Мястото на изпълнение на Услугите по техническа поддръжка се предоставят отдалечено, при необходимост от оказване на съдействие на място е сградата на Министерство на иновациите и растежа в гр. София, ул. „Княз Александър I“ № 12

V. ИЗИСКВАНИЯ КЪМ МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ[2]

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.
2. Във връзка с мрежовата и информационната сигурност на Бенефициера/Възложителя/ МИР/МЕУ 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/Възложителя/ МИР/МЕУ 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 административните органи, които са предмет на защита съгласно приложимото законодателство в областта.

(б) При предоставяне на Услугата спазва правилата за сигурността на информацията на Бенефициера/Възложителя/ МИР/МЕУ. 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/Възложителя/ МИР/МЕУ, подписват декларации по образец на Изпълнителя за опазване на информацията, които се предават на Бенефициера/Възложителя/ МИР/МЕУ. При промяна на лицата в хода на изпълнението съответните подписани декларации се предават, в срок до два работни дни от промяната.

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/Възложителя/ МИР/МЕУ.

4. При неспазване на изискванията за сигурност на информацията Изпълнителят дължи неустойка съгласно уговореното в договора.

5. Лицата, отговорни за мрежовата и информационната сигурност и параметрите на нивото на обслужване при изпълнение на Договора („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 Бенефициера/Възложителя/ МИР/МЕУ;

(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/Възложителя/ МИР/МЕУ;

(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/Възложителя/ МИР/МЕУ, лицата по чл. 10, ал. 2 от НМИМИС съвместно с лицата, които ще имат достъп до системите на МИР от страна на Бенефициера/Възложителя/ МИР/МЕУ и на Изпълнителя

извършват анализ и набелязват мерки за отстраняване на допуснатата нередност в определен срок.