Приложение № 2
към рамков договор № 93-00-97/03.07.2020 г.

ЗАЯВКА по Рамков договор № 93-00-97 от 03.07.2020 г. (вх. № ПО-16-875/03.07.2020 г. на ИО АД)		☒
ЗАЯВКА по Рамков договор № 93-00-97 от 03.07.2020 г. (актуализирана)		☐ [1]
Позиция от ПГ-2026 г.:	*№ по ред от ПГ*	28
Описание на проект съгласно ПГ:	*Решение за защита и инспектиране на DNS трафика*	
CPV код	*48730000-4*	
Рег. номер на писмо от МИДТ за утвърждаване на проекта /становище по проекта	*МИДТ-Рег. № 18-00-260-1/19.11.2026*	
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*	*145 070,00 евро без ДДС*[2]	
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*	*Еднократно, след подписване на Приемо-предавателен протокол (ППП) между Изпълнителя и Бенефициера по чл. 6 от Договора, удостоверяващ приемане на извършените дейности по осигуряване на решение за защита и инспектиране на DNS трафик съгласно Техническите параметри (ТП), копие/я на оторизационно/и писмо/а 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 от датата на подписване на заявката;* *Срок на изпълнение – 36 месеца от дата на осигуряване.*	

[1] Отбелязва се в случай, че заявката е актуализирана

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 подписване на Приемо-предавателен протокол (ППП) между Изпълнителя и Бенефициера по чл. 6 от Договора, удостоверяващ приемане на извършените дейности по осигуряване на решение за защита и инспектиране на DNS трафик съгласно Техническите параметри (ТП) и копие/я на оторизационно/и писмо/а.*
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 страна на БЕНЕФИЦИЕРА:	*Подпис:*
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:	

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

Ръководител на проект по заявката		*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

ТЕХНИЧЕСКИ ПАРАМЕТРИ

за

„Решение за защита и инспектиране на DNS трафика“

гр. София, 2026 г.

I. Цел

Целта на настоящия проект е да бъде осигурено решение за защита и инспектиране на DNS трафика за нуждите на Агенция по вписванията.

DDI / DNS SEC помага за посрещане не изискванията за модернизация на сигурни, устойчиви и гъвкави мрежови основни услуги и DNS сигурност – включително достигане на 100 процента непрекъснатост на бизнеса, предотвратяване на непланирани свързани разходи за нарушения и защита на общественото доверие. Решението помагат на ИТ и SOC екипите да поддържат важно съответствие по отношение на хората, устройствата и системите, които те използват. Използване, подобряване на оперативната ефективност и стимулиране на по-дълбока междуведомствена видимост и цялост на данните.

Предложеното решение е водещият в индустрията доставчик на DNS, DHCP и IPAM (DDI) услуги, отговарящи на нуждите на всяка корпоративна архитектура с решения, базирани на устройства или SaaS, изградени за производителност, мащабируемост, сигурност и надеждност.

II. Обхват на проекта

В обхвата на настоящия проект се включва осигуряване на решение за защита и инспектиране на DNS трафика, което трябва да отговаря на следните минимални технически изисквания:

I. Минимални технически изисквания	
REQ.1	DDI Системата (DNS, DHCP & IP Address Management) трябва да бъде доставена като готов за използване OVA образ с възможност за интегриране във VMware среда.
REQ.2	Системата трябва да предоставя услуга за управление на IP адреси – IPAM (IP Address Management)
REQ.3	Системата трябва да разполага с механизми за контрол на въвежданите данни (коректност на IP адреси, маски и др.)
REQ.4	Системата трябва да позволява добавяне на описания и атрибути за мрежови обекти, IP адреси, домейни. Тези атрибути трябва да имат възможност за дефиниране на типа и размера им
REQ.5	Системата трябва да поддържа механизъм за сканиране на мрежи и хостове/IP адреси (т.нар. network discovery)
REQ.6	Системата трябва да поддържа функции като „намери 10 неизползвани адреса от мрежа X“ и „намери 10 неизползвани подмрежи с размер напр. /24 в подмрежа напр. abcd/16“. Функцията трябва да бъде налична за IPv4 и IPv6
REQ.7	Системата трябва да позволява импортиране на данни в CSV формат директно от графичния интерфейс и да разполага с подробна документация за формата на импортираните данни
REQ.8	Капацитетът на DNS/DHCP/IP базата данни трябва да бъде за минимум 100000 записа.
REQ.9	Системата трябва да позволява интеграция с VMware vCenter и OpenStack услуги, за да извършва процес на откриване на виртуални машини, работещи във VMware/OpenStack инфраструктура, и автоматично да създава DNS записи за тези машини
REQ.10	Системата трябва да поддържа внедряване на DHCP услуги за IPv4 и IPv6 с минимална производителност от 200 DHCP leases в секунда

REQ.11	Системата трябва да поддържа актуализиране на DDNS данни чрез DHCP услугата
REQ.12	Системата трябва да поддържа актуална информация за разпределените IP адреси и устройствата, на които е присвоен даден адрес (MAC адрес, време и дата на присвояване на адреса, IP)
REQ.13	Системата трябва да поддържа функционалност DHCP Failover с възможност за повторно договаряне на наличните адресни пространства
REQ.14	Трябва да бъде възможно проверката за наличност на IP адрес преди неговото разпределяне чрез ICMP
REQ.15	Системата трябва да разпознава типа на устройството/системата на станции, мобилни устройства и др. въз основа на анализа на DHCP заявката. Трябва да поддържа отчет за типа на устройството в историята на DHCP наемите и да предоставя възможност за филтриране/блокиране на разпределението на адреси за избрани типове устройства (напр. разпределяне на адрес за Windows станция, но не и за таблет или смартфон)
REQ.16	Системата трябва да предоставя авторитетни и рекурсивни услуги за разрешаване на домейн имена (DNS - Domain Name System)
REQ.17	Производителността на авторитетния DNS трябва да бъде поне 10 000 DNS заявки в секунда
REQ.18	Системата трябва да изпълнява автоматични DNS актуализации в съответствие с RFC 2136
REQ.19	Системата трябва да разполага с вграден механизъм за уведомяване при промени в зоните, в съответствие с RFC 1996
REQ.20	Системата трябва да поддържа DNS протоколи както за IPv4, така и за IPv6
REQ.21	Системата трябва да поддържа DNS Anycast услуга за IPv4 и IPv6 (използвайки BGP и OSPF протоколи)
REQ.22	Системата трябва да поддържа DNSSEC услуга с автоматично обновяване на подписите при промени в DNS зоните
REQ.23	Системата трябва да поддържа DDNS услуга
REQ.24	Системата трябва да поддържа защитено обновяване на DNS записи с поддръжка на GSS-TSIG протокол
REQ.25	Системата трябва да поддържа MultiMaster DNS функционалност
REQ.26	Системата трябва да поддържа механизъм за IDN (Internationalized Domain Names) и да разполага с вграден конвертор за punycode (поддръжка на кирилица)
REQ.27	Системата трябва да поддържа IDN за DNSKEY записи, DS записи, NSEC записи, NSEC3PARAM записи и RRSIG записи
REQ.28	Системата трябва да поддържа EDNS0 разширения съгласно стандарта RFC 6891
REQ.29	Системата трябва да поддържа следните алгоритми за публични ключове, използвани с DNSSEC: DSA, RSA/MD5, RSA/SHA1, RSA/SHA-256, RSA/SHA-512, ECDSAP/SHA-256, ECDSAP/SHA-384
REQ.30	Подписаните с DNSSEC зони трябва да поддържат динамични DNS актуализации
REQ.31	Системата трябва да поддържа автоматично подписване на DNS записи след промени
REQ.32	Системата трябва да функционира като платформа за разпространение на файлове чрез протоколите TFTP, FTP, HTTP и да предлага услуги за синхронизация на времето чрез NTP (Network Time Protocol)

REQ.33	Системата трябва да работи под контрола на специализирана операционна система. Използването на операционни системи с общо предназначение не е разрешено. Тя не трябва да зависи от или да изисква конкретни версии на операционни системи с общо предназначение или програмни библиотеки
REQ.34	Управлението на системата трябва да се осъществява чрез уеб браузър, без да е необходимо инсталирането на допълнителен софтуер като агент, клиент и др
REQ.35	Възможност за управление от няколко системни администратори, вписани едновременно
REQ.36	Системата трябва да предоставя възможност за управление на IPv4 и IPv6 адреси, позволявайки графичен, конзолен, и API интерфейси
REQ.37	Системата трябва да поддържа удостоверяване на потребители чрез: - Локална потребителска база - RADIUS протокол - TACACS+ протокол - LDAP - Microsoft Active Directory
REQ.38	Системата трябва да има вградена база данни за съхранение на DDI информация. Базата данни не трябва да изисква поддръжка, свързана с нейната конфигурация и управление
REQ.39	Системата трябва да може да бъде наблюдавана чрез SNMP (Simple Network Management Protocol)
REQ.40	Системата трябва да позволява планирани резервни копия (backups) към външен сървър, за да улесни възстановяването в случай на бедствие (чрез TFTP, FTP, SCP)
REQ.41	Системата трябва да поддържа интеграция с инструменти за управление на конфигурацията като Ansible, Puppet и Chef
REQ.42	Системата трябва да поддържа възможност за импортиране и експортиране на данни в различни формати, включително CSV и JSON
REQ.43	Системата трябва да разполага с функционалност за разпознаване и блокиране на DNS тунелиране чрез аналитичен механизъм, базиран на машинно обучение, който разпознава неизвестни модели на тунелиране и извличане на данни чрез DNS. Системата трябва да анализира поне 10 атрибута на всяка DNS заявка, включително: ентропия на символите във FQDN, популярност на дву- и трибуквени комбинации, съотношение на гласни в FQDN, съотношение на цифри, размер на заявката, честота и промяна на честотата на DNS заявките. Системата трябва да открива DNS тунелиране, независимо от категорията на съдържанието на домейна, използван в DNS заявката
REQ.44	В рамките на приемателните тестове, възложителят ще извърши тест за откриване на DNS ексфилтрация. Тестът ще се проведе с персонализиран скрипт, генериращ между 100 и 200 DNS заявки с интервал от 2,5-3,5 секунди
REQ.45	Системата трябва да разполага с функционалност за откриване на прониквания през DNS, по-специално трябва да разпознава техниката, използвана от зловредния софтуер Powersource/DNS Messenger, и да блокира опити за пренос на данни, кодирани в DNS отговори чрез TXT записи
REQ.46	Системата трябва да разполага с функционалност Response Policy Zones (RPZ) за работа като DNS защитна стена въз основа на списъци с опасни домейни

REQ.47	Системата трябва да регистрира и предоставя информация за всички промени, направени от администратори (кой, кога, какво е променил)
REQ.48	Системата трябва да може да изпраща логове към централен хранилищен сървър чрез Syslog механизъм (TCP и UDP)
REQ.49	Системата трябва да позволява администраторите да имат права, базирани на групи и роли, които ограничават достъпа им само до необходимите ресурси. Подробните разрешения трябва да позволяват конфигуриране на права за отделни обекти, като мрежи, DNS зони и конкретни DNS записи.
REQ.50	Системата трябва да поддържа криптирана комуникация между компонентите си чрез TLS (Transport Layer Security)
REQ.51	Достъпът до административния интерфейс трябва да бъде защитен чрез двуфакторна автентикация (2FA)
REQ.52	Системата трябва да предоставя механизъм за защита срещу неоторизиран достъп чрез прилагане на списъци за контрол на достъпа (ACL)
REQ.53	Системата трябва да поддържа защита от атаки тип DDoS срещу DNS и DHCP услуги
REQ.54	Системата трябва да поддържа механизъм за мониторинг и алармиране при откриване на аномалии в мрежовия трафик, свързан с конфигурираните услуги
REQ.55	Системата трябва да има възможност за запис и анализ на потребителските сесии в административния интерфейс за целите на одит и сигурност
REQ.56	Системата трябва да поддържа криптиране на чувствителни данни в конфигурационните файлове и базата данни
REQ.57	Системата трябва да позволява дефиниране на политики за автоматично деактивиране на потребителски акаунти при откриване на подозрителна активност
REQ.58	Системата трябва да има възможност да предприема действия по DNS заявки и отговори въз основа на дефинирани от клиента правила за защита - Възможните действия трябва да включват: разрешаване на заявка без регистриране, разрешаване на заявка с логиране, блокиране на заявка с NXDomain отговор (няма такъв домейн), пренасочване (отговор с дефиниран IP адрес). Пренасочването трябва да е възможно към уеб страница, предоставена от доставчика. Системата трябва също така да позволява пренасочване към всеки IP адрес. - Системата трябва да предприеме действия въз основа на името на домейна в заявката и въз основа на IP адреса в отговора. Действието върху името на домейн трябва да работи за всеки тип заявка – системата не трябва да позволява заобикаляне на блокирането чрез изпращане на специфични типове заявки като SOA или NS. Системата не трябва да позволява заобикаляне на блокирането на злонамерен домейн чрез изпращане на запитвания с главни или смесени FQDN (DNS протоколът е нечувствителен към малки и големи букви, а сигурната DNS система също трябва да е нечувствителна към малки и големи букви - Системата трябва да позволява да се дефинира персонализиран списък с домейни/IP адреси, по които да се действа, и също така трябва да предоставя списък с домейни и IP адреси под формата на емисии за заплахи, дефинирани по-долу. За персонализирани списъци системата трябва да има възможност да дефинира нивото на заплаха и увереността на заплахата за всеки списък. Системата трябва да позволява създаване и

	редактиране на персонализирани списъци от клиентския портал, както и чрез API, за да позволи лесно импортиране на персонализирани данни за заплахи. - Системата трябва да предоставя възможност за заобикаляне на блокове със специфични кодове, предоставени на избрани потребители
REQ.59	Трябва да е възможно изпращането на DNS заявки към услуга предоставяща функции за категоризирането и филтрирането им - от персонализирано дефинирана IP мрежа - от DMZ DNS сървъри, сървърите трябва да добавят вътрешен IP адрес на клиента вътре в заявките и да ги изпращат в криптирана форма към услугата - От роуминг агент, предоставен от доставчика. Роуминг агентът трябва да бъде предоставен за Windows, Mac OS, Android и iOS Данните за заплахите, предоставени от доставчика, трябва да включват - списък на интернет домейни, свързани с APT атаки - списък с домейни и IP адреси, свързани със злонамерен софтуер - Списък с домейни, свързани с рансъмуер - списък с IP адреси, свързани с ботнет мрежи - списък на домейните, свързани със злонамерен софтуер, с помощта на алгоритми за генериране на домейни (DGA) - списък с IP адреси на изходните възли на TOR мрежата - списък с домейни, свързани с фишинг - списък на домейните, свързани с неоторизирано копаене на криптовалута - списък на домейните, регистрирани през последните три дни. Данните за новите регистрации трябва да идват от най-малко 500 различни домейна от първо ниво (домейни от първо ниво). - Списък на домейни, които споделят подозрителни характеристики като примерни домейни, са регистрирани по едно и също време от същия регистрант, който в миналото е регистрирал домейни, за които е доказано, че са свързани със злонамерена дейност
REQ.60	Всички горепосочени списъци за заплахи трябва да бъдат налични за конфигуриране в политиката за защитени DNS услуги, както и във формат RPZ, за да бъдат изтеглени на DNS сървъритею
REQ.61	Списъците за заплахи от доставчика трябва да бъдат достъпни чрез API във формати CSV, STIX, XML, JSON и CEF за използване в други системи за сигурност като SIEM, защитни стени или защитени уеб шлюзове
REQ.62	Разузнаването на заплахите трябва да може да предоставя контекстуална информация за домейн/IP, поне трябва да включва данни, ако заплахата е свързана с ексфилтрация на данни, влияе ли върху наличността на системите, необходимо ли е взаимодействие с потребителя за активиране на заплахата, какви техники са включени
REQ.63	Защитената DNS услуга трябва да има функционалност за откриване на непознати DGA и DGA домейни в DNS заявки
REQ.64	Защитената DNS услуга трябва да има информация за категорията съдържание за домейни и трябва да може да действа по нея, например трябва да предоставя възможност за предприемане на действия за домейни, хостващи съдържание като порно, опасност, социални мрежи, анонимайзери и др.
REQ.65	Системата трябва да поддържа механизми за висока наличност (High Availability - HA) за всички основни услуги, включително DNS, DHCP и

	IPAM
REQ.66	Системата трябва да поддържа клъстеризация на компонентите си с цел осигуряване на надеждност и отказоустойчивост
REQ.67	Системата трябва да позволява автоматично превключване (failover) при отпадане на даден сървър или услуга
REQ.68	Системата трябва да поддържа географски разпределено внедряване с възможност за репликация на данни между различни локации
REQ.69	Системата трябва да има механизъм за автоматично балансиране на натоварването (load balancing) между DNS и DHCP сървърите
REQ.70	Системата трябва да осигурява непрекъсната работа при актуализации (Rolling Updates), без да се нарушава функционирането на критичните услуги
REQ.71	Системата трябва да позволява възстановяване след срив (Disaster Recovery) чрез механизъм за архивиране и репликация на данни
REQ.72	Системата трябва да поддържа синхронизация на конфигурацията и данните между главните и резервните инстанции в реално време
REQ.73	Бързо възстановяване на услугите в случай на срив, като времето за възстановяване не трябва да надвишава 10 минути.
REQ.74	Системата трябва да предоставя централизирана отчетност за всички DNS, DHCP и IPAM събития
REQ.75	Системата трябва да поддържа механизъм за събиране и анализ на логове, включително възможност за интеграция с SIEM (Security Information and Event Management) решения
REQ.76	Системата трябва да позволява генериране на персонализирани отчети за използването на IP адреси, DHCP лизинги и DNS заявки
REQ.77	Системата трябва да осигурява механизъм за известяване на администраторите чрез имейл, SNMP трап (trap) или уеб интерфейс при откриване на критични събития
REQ.78	Системата трябва да предоставя детайлни статистики за производителността на DNS и DHCP услугите, включително натоварване, време за отговор и брой заявки
REQ.79	Системата трябва да позволява интеграция със системи за мрежов мониторинг чрез SNMP (v2c и v3)
REQ.80	Системата трябва да предоставя исторически данни за заетостта на IP адресите и тенденциите на използване
REQ.81	Системата трябва да поддържа механизъм за автоматично архивиране на логове и отчети за последващ анализ
REQ.82	Системата трябва да позволява конфигуриране на политики за съхранение и изтриване на исторически данни
REQ.83	Системата трябва да може да визуализира информацията чрез графики и диаграми в уеб интерфейса
REQ.84	Порталът за защитени DNS услуги трябва да предоставя възможности за отчитане. Докладите трябва да включват: - Отчети за дейността, показващи DNS заявки, изпратени до услугата - Отчети за защитата, показващи DNS заявки, които засягат правилата за сигурност - Трябва да има възможност за изпращане на изходни данни (заявки, събития за защита) до локална SIEM система под формата на съобщения в системен дневник или директна интеграция
REQ.85	Достъпът до клиентския портал трябва да се основава на потребителски данни за вход със специфични роли за достъп, като например достъп само за четене или административен достъп. Промените в

	конфигурацията на DNS услугата трябва да бъдат регистрирани в регистрационния файл за проверка.
REQ.86	Висока производителност с минимално време за отговор на DNS заявки (не по-високо от 50 милисекунди) при натоварване до 5 хиляди заявки на секунда.
REQ.87	Поддържка на DHCP услуги с производителност минимум 200 заявки на секунда.
REQ.88	Надеждност при обработка на големи обеми данни и да не претоварва мрежовата инфраструктура при високи натоварвания.
REQ.89	Възможност за работа с разширени DNS записи и поддържа функционалности като DNSSEC и Anycast без да се нарушава производителността.
REQ.90	Възможност за обработка на натоварвания, които включват обработка на над 30 милиона DNS заявки и DHCP лизинги месечно.
REQ.91	Възможност за динамично регулиране на ресурсите според натоварването, включително за работа в облачни среди и виртуализирани инфраструктури.
REQ.92	Възможност за интелигентно управление на натоварването и оптимизация на ресурсите чрез използване на технологии като load balancing и autoscaling.
REQ.93	Да бъде в състояние да обслужва нуждите на организацията при неограничено нарастващ обем от мрежови услуги и данни, като остава стабилна и ефективна.
REQ.94	Системата трябва да е лицензирана за минимум 850 потребителя.
REQ.95	DDI Системата трябва да е оразмерена и лицензиране лицензирана за безпроблемна работа на поне 1000 IP адреса.
	Гаранция и поддръжка
REQ.96	Поддръжка от производителя, включително получаване на нови версии на софтуера и 24/7 техническа помощ чрез телефон, имейл и портал за заявки за срок от минимум 3 (три) години.

II. Изисквания към изпълнението

Изпълнителят следва да осигури решението от лице, надлежно оторизирано от производителя или официален негов представител за предоставяне на право на продажба/разпространение на предлаганите софтуерни продукти на територията на Република България.

При доставка на софтуерното решение трябва да е осигурена последната актуална версия на софтуерните продукти към датата на доставката.

Доставените лицензи в рамките на софтуерното решение за защита и инспектиране на DNS трафика трябва да са на името на Агенция по вписванията.

Провеждане на обучение за работа със софтуера, запознаване с решението под формата на презентация за служители на дирекция ИОТ, в рамките на до 4 часа. Решението ще се имплементира със съдействие на служители на Агенция по вписванията.

III. Място на изпълнение

Мястото на изпълнение на дейностите е гр. София, ул. „Елисавета Багряна“ № 20.

IV. Изисквания към мрежовата и информационната сигурност[3]

4.1 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.

4.2 Във връзка с мрежовата и информационната сигурност на Бенефициера (АВ) 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 (АВ), ще спазват изискванията за сигурността на информацията съгласно Закона за киберсигурност и НМИМИС.

(б) При предоставяне на Услугата спазва правилата за сигурността на информацията на Бенефициера (АВ). 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 (АВ), подписват декларации по образец на Изпълнителя за опазване на информацията, които се предават на Бенефициера (АВ). 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 (АВ) 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.

4.3 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 (АВ).

4.4 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;

---

[3] 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 (АВ), които са предмет на защита съгласно приложимото законодателство в областта.

(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 (АВ);

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