

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.:	<i>№ по ред от ПГ</i>	15
Описание на проект съгласно ПГ:	„Осигуряване на системата за защита на вътрешните мрежи от изтичане на критична информация (DLP) “*	
CPV код	72000000-5	
Рег. номер на писмо от МИДТ за утвърждаване на проекта /становище по проекта	МИДТ-33-00-71/16.07.2026	
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	198 210,00 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 осигуряването на системата за защита на вътрешните мрежи от изтичане на критична информация (DLP) 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	НЕПРИЛОЖИМО	

¹ Отбелязва се в случай че заявката е актуализирана

дата или в месеци, ако не е обвързан с конкретна дата)		
Отчитане: (периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)	Еднократно, с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ осигуряването на системата за защита на вътрешните мрежи от изтичане на критична информация (DLP).	
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:

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

Ръководител на договора от страна на БЕНЕФИЦИЕРА:		<i>Подпис:</i>
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:		
Ръководител на проект по заявката		<i>Подпис:</i>
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД		<i>Подпис:</i>

**Заявката се подписва под условие и ще бъде изпълнена при осигурено финансиране от страна на Бенефициера, като същият надлежно уведомява Изпълнителя*

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

ТЕХНИЧЕСКИ ПАРАМЕТРИ

за

„Осигуряване на системата за защита на вътрешните мрежи от изтичане на критична информация (DLP)“

Гр.София, 2026г

1. ЦЕЛ

Целта на заявката е осигуряване на системата за защита на вътрешните мрежи от изтичане на критична информация (DLP) за нуждите на Национален осигурителен институт (НОИ), различна от доставената по Договор № BG16RFPR002-2.018-0001-S01/06.11.2025 г. „Повишаване на националните способности за координация и реагиране при инциденти, свързани с киберсигурността“.

2. ОБХВАТ

В обхвата на заявката се включва осигуряване на решение за предотвратяване на изтичане на данни от крайни точки за нуждите на Национален осигурителен институт (НОИ), което трябва да отговаря на следните минимални технически изисквания:

Минимални технически изисквания	
REQ. 1.	Предложеното решение трябва да включва лицензи за 3950 Windows-базирани крайни точки и 50 Linux-базирани крайни точки. Предложените лицензи трябва да са с валидност и включена поддръжка за период от 36 месеца.
REQ. 2.	Решението трябва да може да предпазва крайни точки от изтичане на данни и трябва да е съвместимо минимално със следните операционните системи: Windows.
REQ. 3.	Функциите на решението за защита от изтичане на данни трябва да са еднакви, независимо от вида на защитените операционни системи.
REQ. 4.	Решението трябва да поддържа минимално: -всички Windows операционни системи, които са текущо поддържани от Microsoft; -актуално поддържани дистрибуции на Linux от тип Ubuntu и Red Hat Enterprise;
REQ. 5.	Решението трябва да разполага минимално с компоненти на ниво крайна точка за защита на ниво съдържание и за управление на преносими устройства за данни.
REQ. 6.	Решението трябва да разполага със собствена база от данни или да може да се интегрира минимално с MySQL база от данни.
REQ. 7.	Решението трябва да може да се поставя под формата на хардуерно или виртуално устройство. Да се поддържат минимално следните виртуални дистрибуции за виртуално устройство: VMware, Hyper-V, Oracle VM VirtualBox, Citrix XenServer.
REQ. 8.	Решението трябва да може да се интегрира и синхронизира с директорийни услуги, минимално Активна директория и Entra ID.
REQ. 9.	Клиентският софтуер на решението, за поставяне по крайните точки, трябва да може да се дистрибутира минимално чрез Активна директория и груповата политика, чрез Jamf и чрез Microsoft Intune.
REQ. 10.	Решението трябва да разполага с централизирана конзола за управление, достъпна през уеб-браузър.

REQ. 11.	Решението трябва да позволява изграждане и поставяне на политики и правила за управление и защита минимално на индивидуални устройства, потребители, групи от потребители, глобални правила за всички защитени крайни точки.
REQ. 12.	Решението трябва да разполага с изглед с описание на всички управлявани преносими устройства с тяхното име, тип, сериен номер, статус (забранено, позволено, лимитирано устройство). Този изглед трябва да предоставя възможност за преглед, сортиране и извличане на списъци с данни минимално в Excel, PDF и CSV формат.
REQ. 13.	Решението трябва да позволява вмъкването и извличането на списъци с преносими устройства в JSON формат или директно от Активна директория.
REQ. 14.	Решението трябва да разполага минимално със следните политики за управление на преносими устройства: -позволен достъп -забранен достъп -достъп само за четене на информация -позволен достъп само при определени нива на доверие на устройство -позволен достъп само в определени работни часове -политики за достъп според мрежовата локация (в или извън мрежата на организацията) на устройствата.
REQ. 15.	Решението трябва да поддържа минимално следните типове преносими устройства: • Преносими устройства за съхранение на данни • Стандартни USB флашки, U3 и Autorun устройства • USB 1.1, USB 2.0, USB 3.0 устройства • Карти памет - SD, MMC, Compact Flash • Четци за карти • CD/DVD-Player/Burner • Дигитални камери • Смартфони / Handheld устройства / Персонални дигитални асистени (минимално Nokia N-Series, Blackberry, Windows CE съвместими устройства, Windows мобилни телефони) • iPod / iPhones / iPad устройства • MP3 Player / Media Player устройства • Външни твърди дискове (HDD) / преносими твърди дискове • FireWire устройства • PCMCIA устройства • Биометрични устройства • Bluetooth устройства • Принтери (минимално за свързани чрез сериен порт, USB, LTP методи) • Express Card (SSD) • Безжични USB устройства • LPT/Паралелен порт за устройства за съхранение на данни • Флопи диск устройства • Serial ATA контролери • Мрежови устройства.
REQ. 16.	Решението трябва да може да защитава RDP файловия трансфер на терминални сървъри и тънки клиенти.

REQ. 17.	Решението трябва да разполага с изглед с всички защитени компютърни устройства минимално с данни за тяхното име, IP адрес, MAC адрес, домейн, работна група, сериен номер или ID, операционна система.
REQ. 18.	Решението трябва да позволява филтриране на изгледа с компютърни устройства по различни показатели, с възможност за ръчно добавяне на ново устройство или вмъкване на компютърни устройства от Активна директория. Този изглед трябва да позволява премахването на клиентския софтуер на решението от дадено компютърно устройство и възможност за изтриване на устройство от списъка.
REQ. 19.	Решението трябва да може да обвързва компютърни устройства с вписани в тях потребители и да предоставя данни за потребителското име в изгледа с компютърни устройства.
REQ. 20.	Решението трябва да може автоматично да засича потребителите, които се вписват в защитените устройства и да разполага със списък с всички потребители.
REQ. 21.	Трябва да могат да се вмъкват потребители ръчно и чрез Активна директория, като минимално да могат да се въведат потребителски данни за тяхното потребителско име, първо име, фамилия, отдел, данни за контакт.
REQ. 22.	Решението трябва да може автоматично да мониторира и съхранява всички потребителски действия с данни и да предоставя изглед с история на действията на даден потребител.
REQ. 23.	Решението трябва да позволява групиране на потребители и компютърни устройства за поставяне на политики за сигурност. Групите трябва да могат да се създават ръчно или да се вмъкват от Активна директория.
REQ. 24.	Решението трябва да може автоматично да групира потребители и компютърни акаунти в динамични групи според избрани индикатори (например по име, ID и други), като да може да се избира интервалът на синхронизиране на динамичните групи минимално в зададен брой минути.
REQ. 25.	Решението трябва да може да открива и защитава лични данни (PII), финансови данни и данни от кредитни карти, конфиденциални файлове.
REQ. 26.	Решението трябва да разполага с OCR механизъм за разпознаване на изображения за откриване на чувствителна информация в тях.
REQ. 27.	Решението трябва да може да мониторира и контролира трансфера на данни, минимално за трансфери: -към преносими устройства и други медийни устройства -в локалната мрежа (споделени мрежови дялове) -в Интернет, минимално чрез email клиенти, приложения за споделяне на файлове, уеб браузъри, Instant Messaging платформи, социални медии -към облачни среди, минимално iCloud, Google Drive, Dropbox, Microsoft SkyDrive -чрез клипборд (минимално за Copy/Paste и Cut/Paste операции) -чрез Print Screen операции -чрез принтери
REQ. 28.	Решението трябва да може да блокира принтиране на уеб страници минимално за следните уеб-браузъри: Internet Explorer, Mozilla Firefox, Google Chrome, Safari, Opera.
REQ. 29.	Решението трябва да разполага с функция за извличане и засичане на съдържание от мрежовия трафик от защитени крайни точки, прозрачно или чрез пренасочване към прокси сървър.
REQ. 30.	Решението трябва да предлага възможност за блокиране на трансфера на

	данни за Bluetooth връзки, дори за устройства, които вече са сдвоени. Тази функция трябва да е налична минимално за защитени Windows-базирани крайни точки.
REQ. 31.	Решението трябва да разполага с функция за игнориране на виртуални принтери за подобряване на производителността, минимално за Microsoft to PDF и PDFCreator.
REQ. 32.	Решението трябва да позволява конфигуриране на максималния обем на анализирани от решението файлове, с възможност за определяне на обем на файл в диапазон от 1KB до 4GB.
REQ. 33.	Решението трябва да позволява задаването на лимит на броя трансфери на данни за определен часови диапазон, с опции минимално за мониториране или блокиране при прехвърляне на зададения лимит.
REQ. 34.	Решението трябва да може да открива и защитава съдържание в новия Outlook чрез Microsoft 365 Web Add-in.
REQ. 35.	Решението трябва да може да открива и защитава съдържание при работа с LLM модели за изкуствен интелект, минимално за ChatGPT, Microsoft Copilot, Google Gemini, DeepSeek, X Grok и Claude.
REQ. 36.	Решението трябва да разполага с функция за задаване на временна офлайн парола (например когато няма мрежова свързаност между защитени компютри и контролера на решението) за временен пълен достъп до данните на дадена крайна точка, на ниво дадено устройство или на ниво даден потребителски акаунт. Минимално да има възможност за задаване на периода на валидност за определени минути, часове или дни. Трябва да има възможност за добавяне на бележка за причината за създаване на временна парола.
REQ. 37.	Решението трябва да разполага с функции за създаване на отчети за процеси с трансфер на файлове и за работа с чувствително съдържание. Трябва да има възможност за извличане на отчети минимално в Excel, PDF и CSV формат.
REQ. 38.	Решението трябва да позволява задаването и изпращането на аларми за различни действия, минимално по email до конкретни лица.
REQ. 39.	Решението трябва да предлага възможност за настройване на Single Sign On метод на вписване в конзолата на решението, минимално чрез OKTA и Entra ID.
REQ. 40.	Решението трябва да разполага с функция за бекъпиране и възстановяване на конфигурацията на данните на решението, както ръчно, така и автоматично. Ключът за бекъпиране не трябва да се съхранява в самото решение от съображения за сигурност.
REQ. 41.	Решението трябва да разполага с функция за изпращане файлове „сенки“ към външни за крайните точки локации.
REQ. 42.	Решението трябва да спомага за съответствие с изискванията на различни стандарти, минимално ISO27000, PCI-DSS, NIST.
Гаранция и поддръжка:	
REQ. 43.	Период на поддръжка: минимум 36 (тридесет и шест) месеца
REQ. 44.	Възможност за обновление на софтуера в периода на поддръжката до последна актуална версия на производителя.

3. МЯСТО НА ДОСТАВКА И ПОДДРЪЖКА

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

3.2. Услугите по техническа поддръжка се предоставят отдалечено, като при необходимост от оказване на съдействие на място, мястото на изпълнение е в сградата на Национален осигурителен институт – гр. София, бул. „Ал. Стамболийски” № 62-64.

4. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО

- Изпълнителят следва да осигури решението от лице, надлежно оторизирано от производителя или официален негов представител за предоставяне на право на разпространение/доставка на предлаганите софтуерни продукти на територията на Република България.
- В случай на установени проблеми или инциденти, които попадат в обхвата на техническата поддръжка, лицето, установило проблема, регистрира заявка за проблем/инцидент в система за управление на заявки (СУЗ), осигурена от Изпълнителя. Всички заявки за наличие на проблем или инцидент трябва да се регистрират в системата за управление на заявки, дори да са получени чрез друг комуникационен канал – електронна поща или телефон.

5. ИЗИСКВАНИЯ КЪМ МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ²

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) и които ще имат достъп до информация, информационни активи, системи и/или инфраструктура на Бенефициера (НОИ), при взаимодействието си със служители на Бенефициера (НОИ), ще спазват изискванията за сигурността на информацията съгласно Закона за киберсигурност и НМИМИС.

(б) При изпълнение на Услугата спазва правилата за сигурност 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 настъпване на промяната.

(в) определя компетентното лице, отговорно за мрежовата и информационна сигурност, което осъществява взаимодействие с компетентно лице от страна 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.

Бенефициера (НОИ), включително при възникване, управление и докладване на инцидент по МИС.

(г) осигурява адекватни 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 на данните и предотвратяване на изтичане на критична информация. Имплементираните смекчаващи механизми трябва да са пропорционални на установените рискове и на потенциалните щети, които биха могли да настъпят за Бенефициера (НОИ), включително по отношение на конфиденциалност, цялостност и наличност на информацията.

5.3 Изпълнителят се задължава да не разпространява информация, станала му известна при или 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 комуникация и координация 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 на адекватни мерки за мрежова и информационна сигурност от страна на Изпълнителя (и на подизпълнителите, когато е приложимо);

(в) При получена информация за инцидент, нарушение, отклонение или събитие, което може да доведе до нерегламентиран достъп, изтичане на критична информация или компрометиране на DLP системата, лицата по чл. 10, ал. 2 от НМИМИС осъществяват незабавна комуникация по телефон и/или имейл и предприемат действия за анализ на: причините за възникване на инцидента или 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 (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 мерки за отстраняване на допуснатите несъответствия в определен срок.