Приложение № 2
към рамков договор № 15/05.08.2025 г.

ЗАЯВКА по Рамков договор № ДОГ-00-160/21.10.2025 г. **(№ ПО-16-2761/04.11.2025 на ИО АД)**	☒
ЗАЯВКА по Рамков договор № ……...2025 г. **(актуализирана)**	☐ [1]

Позиция от ПГ-2025 г.:	*№ по ред от ПГ*	*1*
Описание на проект съгласно ПГ:	*Обследване на използваните информационни и комуникационни системи в ДА Архиви*	
CPV код	*72700000-7*	
Рег. номер на писмо от МЕУ за утвърждаване на проекта /становище по проекта	*№ МЕУ-19892/22.12.2025*	
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*	***19 500,00 лв. 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 извършените дейности по обследване на използваните информационни и комуникационни системи в ДА Архиви* *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 авансовото плащане с вкл. ДДС и издадена фактура.*
Плащане с акредитив ДА/НЕ	*Не*
Документи за плащане с акредитив	*Не е приложимо.*
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*До 4 месеца след подписване на заявката.*
Гаранционен срок: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*Съгласно техническите параметри.*
Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*	*Еднократно, с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ извършените дейности по обследване на използваните информационни и комуникационни системи в ДА Архиви*
Приложения: (*напр: технически параметри, образци на отчетни*	*Технически параметри.*

[1] Отбелязва се в случай че заявката е актуализирана

документи)		
Настоящата заявка да се изпълни при условията на приложените Технически параметри.		
ЗАЯВКАТА е ИЗГОТВЕНА ОТ:		
Ръководител на проект по заявката от страна на БЕНЕФИЦИЕРА (напр: представител на дирекцията – Заявител):		*Подпис:*
ЗАЯВКАТА е ОДОБРЕНА ОТ:		
Координатор на договора от страна на ВЪЗЛОЖИТЕЛЯ:		*Подпис:*
Ръководител на договора от страна на БЕНЕФИЦИЕРА:		*Подпис:*
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:		
Ръководител на проект по заявката		*Подпис:*
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД		*Подпис:*

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

ТЕХНИЧЕСКИ ПАРАМЕТРИ

ЗА

ОБСЛЕДВАНЕ НА ИЗПОЛЗВАНИТЕ ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ СИСТЕМИ В ДА АРХИВИ

1. ПРЕДМЕТ

В предмета на заявката се включва дейности по обследване на използваните информационни и комуникационни системи в ДА архиви .

2. ОБХВАТ

По време на преглед експерти от „Информационно обслужване“ АД (ИО АД) ще следват принципи, регламентирани в международни стандарти. За събиране на необходимата информация, експертите на ИО АД ще използват наличната документация и ще изискват преглед на текущата конфигурация.

Дейности в обхвата

a. Преглед на мрежови системи

- Политики за управление на мрежовите системи
- Топология на комуникационните трасета
- Анализ на мрежови сегменти, устройства и системи
- Анализ на мрежови сегменти
- Периметър на мрежата
- Опорна мрежа
- Сървърни и системни мрежи
- Ниво на достъп и потребителска мрежа
- Анализ на отдалечения достъп
- Анализ на система за наблюдение наличността на комуникационни устройства и мрежовите връзки
- Анализ на системи за мрежова сигурност
- Анализ на защитни стени
- Анализ на система за защита от DDoS атаки
- Анализ на IPS/IDS системи
- Анализ на прокси сървъри
- Анализ на безжични мрежи

b. Преглед на сървърни системи

- Политики за управление
- Анализ на Linux системи
- Анализ на Windows системи
- Анализ на Активна директория (MS AD)
- Анализ на потребителите с административни и/или системни права
- Анализ на възникналите и потенциалните проблеми при репликиране между домейн контролерите
- Анализ на състоянието на дялове за данни на Активната директори

- Анализ на топологията на използваната Активна директория топология на Forest ниво. Domain ниво и репликациите между домейн контролерите
- Анализ на инсталирания софтуер върху домейн контролерите на Активната директория
- Анализ на хубавите политики в Активната директория
- Анализ на електронна пощенска услуга
- Анализ на конфигурацията и параметрите за надеждност и сигурност на пощенската услуга
- Анализ на системи за защита на пощенската услуга
- Анализ на система за защита на крайни хостове (АУ. EDR)

c. Преглед на дискови системи

- Политики за управление
- Анализ на комуникационна среда
- Анализ на дискови групи
- Анализ на дисков капацитет

d. Преглед на системи за управление на бази данни

- Политики за управление
- Анализ на системи за управление на бази данни
- Анализ на приложни системи

e. Преглед на системи за резервиране и възстановяване на данни и информация

- Политики за управление
- Анализ за резервиране и възстановяване на виртуални машини, бази данни, файлове и данни

f. Преглед на системи за мониторинг

- Анализ на ИТ ресурси и услуги, които се наблюдават
- Анализ на зададените гранични стойности
- Анализ на групите потребители. които се известяват

g. Сканиране за технически уязвимости

- Сканиране за технически уязвимости на всички публично достъпни ИТ услуги
- Сканиране за технически уязвимости на всички ИТ ресурси в локалните мрежи

В резултат от изпълнението на гореописаните дейности ще бъдат изготвени и предоставени следните документи:

- Подробен технически доклад за текущото състояние на ИКИ на ДА архиви.
- Препоръки за подобряване на производителността на ИКИ и повишаване на нивото на информационната сигурност на ресурсите и информацията в ИКИ в ДА архиви.

3. МЯСТО НА ИЗПЪЛНЕНИЕ

Сградата на ДА архиви , в гр. София, ул. „Московска“ №5

4. ИЗИСКВАНИЯ КЪМ МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ[2]

[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 Възложителя/Бенефициера (МЕУ/ДАА), които са предмет на защита съгласно приложимото законодателство в областта.

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 Възложителя/Бенефициера (МЕУ/ДАА) 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 Възложителя/Бенефициера (МЕУ/ ДАА), 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 Възложителя/Бенефициера (МЕУ/ ДАА). 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 Възложителя/Бенефициера (МЕУ/ ДАА), подписват декларации по образец на Изпълнителя за опазване на информацията, които се предават на Възложителя/Бенефициера (МЕУ/ ДАА). 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 Възложителя/Бенефициера (МЕУ/ ДАА) 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.

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 Възложителя/Бенефициера (МЕУ/ ДАА).

4. 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 съответната администрация;

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

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

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