

ЗАЯВКА по Договор № РД-06-43 от 07.06.2021 г.		<input checked="" type="checkbox"/>
(вх. № ПО-16-2554/08.06.2021 г. на „Информационно обслужване“ АД)		
ЗАЯВКА (актуализирана)		<input type="checkbox"/> ¹
Позиция от ПГ-2024 г.:	<i>№ по ред от ПГ</i>	7
Описание на дейност/проект съгласно ПГ:	<i>Преглед на информационната и комуникационна инфраструктура на Изпълнителна агенция „Медицински надзор“ (ИАНН)</i>	
CPV код	72820000-4	
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 кредитив/ авансово	5 000,00 лв.	
Начин за плащане: (еднократно, на части, периодично или др.)	Еднократно, след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на изпълнението на услугата с приложени документи по т. 3 от техническите параметри към заявката и издадена фактура.	
Плащане с кредитив или авансово ДА/НЕ	НЕ	
Документи за плащане с кредитив или авансово	Не е приложимо	
Срок на изпълнение: (от дата – до дата или в месеци, ако не е обвързан с конкретна дата)	Срок за изпълнение - до 30 работни дни от подписване на заявката	
Гаранционен срок: (от дата – до дата или в месеци, ако не е обвързан с конкретна дата)	Не е приложимо	
Отчитане: (периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)	Еднократно, с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на изпълнението на услугата с приложени документи по т. 3 от техническите параметри към заявката.	
Приложения: (напр: технически параметри, образци на отчетни документи)	Технически параметри	
Настоящата заявка да се изпълни при условията на приложените Технически параметри.		
ЗАЯВКАТА Е ИЗГОТВЕНА И СЪГЛАСУВАНА ОТ:		
Координатор по заявката:		

¹ Отбелязва се в случай че заявката е актуализирана

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

<p>Ръководител на проект/дейност по заявката (напр: представител на дирекцията – Заявител):</p>		
<p>ЗАЯВКАТА е ОДОБРЕНА ОТ:</p>		
<p>Ръководител на договора от страна на ВЪЗЛОЖИТЕЛЯ:</p>		
<p>ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:</p>		
<p>Координатор от „Информационно обслужване“ АД по заявката</p>		
<p>Ръководител на проект/дейност по заявката</p>		
<p>Ръководител по изпълнението на Договора от „Информационно обслужване“ АД</p>		

ТЕХНИЧЕСКИ ПАРАМЕТРИ

ЗА ПРЕГЛЕД НА ИНФОРМАЦИОННАТА И КОМУНИКАЦИОННА ИНФРАСТРУКТУРА НА ИЗПЪЛНИТЕЛНА АГЕНЦИЯ „МЕДИЦИНСКИ НАДЗОР“

1. Цел

Извършване на преглед на информационната и комуникационна инфраструктура на Изпълнителна агенция „Медицински надзор“ (ИАМН) и даване на препоръки за подобряване на производителността на ИКИ и повишаване на нивото на информационната сигурност на ресурсите и информацията в ИКИ.

2. Обхват

2.1. Подход при провеждане на прегледа

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.

2.2. Дейности в обхвата

2.2.1. Преглед на поддържащи ИКИ системи:

2.2.1.1. Инфраструктура;

- Анализ на техническите помещения;
- Анализ на структурна кабелна система;

2.2.1.2. Електрозахранване;

- Анализ на система за осигуряване на аварийно захранване;
- Анализ на система за осигуряване на непрекъсваемо захранване;

2.2.1.3. Системи за контрол на околната среда;

- Анализ на система за осигуряване ОВК;
- Анализ на система за мониторинг на околната среда;

2.2.1.4. Системи за сигурност;

- Анализ на система за контрол на достъпа;
- Анализ на система против проникване;
- Анализ на система за видеонаблюдение;
- Анализ на система за пожароизвестяване;
- Анализ на система за пожарогасене;

2.2.2. 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 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;
- Анализна система за защита от DDoS атаки;
- Анализ на IPS/IDS системи;
- Анализ на прокси сървъри;
- Анализ на безжични мрежи;

2.2.3. 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 директория;
- 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 груповите 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);

2.2.4. Преглед на дискови системи;

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

2.2.5. Преглед на системи за управление на база данни;

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

2.2.6. Преглед на приложни системи

- Политики за управление
- Анализ на приложни системи
- Изготвяне на технически паспорт за всяка идентифицирана приложна система

2.2.7. Преглед на системи за резервиране и възстановяване на данни и информация;

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

2.2.8. 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;

2.2.9. Сканиране на технически уязвимости;

- Сканиране за технически уязвимости на всички публично достъпни ИТ услуги;
- Сканиране за технически уязвимости на всички ИТ ресурси в локалните мрежи;
- Анализ на системи за сигурност;
- Анализ на политики за сигурност;
- Анализ на модел за защита в организацията.

3. Резултати

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

3.1. Подробен технически доклад за текущото състояние на ИКИ;

3.2. Препоръки за подобряване на производителността на ИКИ и повишаване на нивото на информационната сигурност на ресурсите и информацията в ИКИ.

4. Място на изпълнение

Мястото на изпълнение е сградата на ИАМН, на адрес: гр. София, ул. „Св. Георги Софийски“ № 3.