Приложение № 2
към рамков договор № № ПО 16-3109/11.10.2024 г.

ЗАЯВКА по Рамков договор № № ПО 16-3109 от 11.10.2024 г.	☑
ЗАЯВКА по Рамков договор № ПО 16-3109 от 11.10.2024 г. (актуализирана)	☐ [1]

Позиция от ПГ-2026 г.:	*№ по ред от ПГ*	*6*
Описание на проект съгласно ПГ:	*Доставка на хардуерни и софтуерни ресурси* *Дейност 2 – Доставка на хардуерни и софтуерни ресурси за 2026 г.*	
CPV код	*48600000-4*	
Рег. номер на писмо от МЕУ за утвърждаване на проекта /становище по проекта	*МИДТ Рег. № 92-00-388/24.07.2026г.*	
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*	*182 360,00 евро*
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*	*На части, след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на всяка извършена доставка/услуга по съответната дейност 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***)**	*До 30.10.2026 г.*
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)*	*На части, с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на всяка извършена доставка/услуга по съответната дейност и издадена фактура.*
Приложения: (*напр: технически параметри, образци на отчетни документи*)	*Технически параметри*
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:	

[1] Отбелязва се в случай че заявката е актуализирана

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:*

Забележка: *С една заявка могат да се възлагат повече от един проект по ПГ, само когато те са еднотипни и управлението им (възлагане, изпълнение, отчитане) може да се извършва съгласно описаните в таблицата от заглавната страница на заявката параметри и лица. В този случай в таблицата се добавят необходимия брой редове, за описване на съответните проекти. Когато проектите не са еднотипни, те се възлагат с отделни заявки.*

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

ТЕХНИЧЕСКИ ПАРАМЕТРИ

ЗА

ДОСТАВКА НА ХАРДУЕРНИ И СОФТУЕРНИ РЕСУРСИ

ЗА

СМЕТНАТА ПАЛАТА НА РЕПУБЛИКА БЪЛГАРИЯ

1. ЦЕЛ

Целта на заявката е да се осигурят хардуерни и софтуерни ресурси за нуждите на Сметна палата на Република България.

2. ОБХВАТ

В обхвата на заявката са включени следните дейности:

2.1. Доставка на специализиран дисков масив за архиви със следните минимални технически изисквания:

Минимални технически изисквания	
REQ.1	Количество: 1 брой
REQ.2	Тип на шасито – за вграждане в 19-инчов шкаф.
REQ.3	Капацитет – минимум 40TB използваем капацитет преди компресия и дедупликация, с възможност за бъдещи разширения до 250TB.
REQ.4	Устройството трябва да разполага с мин. 4 порта със скорост 25 Gb/s със съответните SFP модули и мин. 2 порта със скорост 1 Gb/s.
REQ.5	Данните да могат да се изпращат по LAN, като се използват CIFS, NFS, NDMP протоколи.
REQ.6	Да поддържа изпращане на данните през SAN/FC (Storage Area Network/Fibre Channel), чрез добавяне само на комуникационни модули
REQ.7	Всички методи за комуникация изброени в REQ.4 и REQ.5 да могат да работят едновременно.
REQ.8	Устройството/системата трябва да поддържа Inline дедупликация на данните.
REQ.9	Устройството/системата трябва да поддържа употребата на софтуерни приставки (plug-ins) на backup сървъра/медия сървъра/storage устройството/backup клиента, които да позволяват дедупликация на данните преди изпращането им към backup устройството.
REQ.10	Устройството трябва да поддържа криптиране при репликация.
REQ.11	Устройството трябва да поддържа репликация на дедуплицираните данни към същия или подобен тип устройство.
REQ.12	Устройството трябва да поддържа архивиране (backup) на данните с възможност за заключване на архивираните файлове (retention lock)
REQ.13	Устройството трябва да поддържа моментни копия/snapshots.
REQ.14	Устройството да поддържа виртуална лентова библиотека.
REQ.15	Устройството да поддържа глобална дедупликация на всички пространства (CIFS/NFS shares, VTL, различни директории и др.).
REQ.16	Устройството да поддържа: - Retention lock compliant with SEC 17a-4(f) - Dual Role Authorization (Admin & Security Officer) - Secure System Clock, NTP Clock Tamper Controls - Multi-factor Authentication - Support for snapshots - Data Invulnerability Architecture (Continuously checks Data Written is data stored – Self Healing)

REQ.17	Гаранционна поддръжка – минимум 36 месеца хардуерна поддръжка от производителя.

2.2. Доставка на софтуер за архивни копия със следните минимални технически изисквания:

Минимални технически изисквания	
REQ.1	Да осигурява резервни копия както на виртуалната среда, така и на физически машини
REQ.2	Решението трябва да включва всички необходими компоненти и лицензи за бекъп на: операционни системи, бази данни и др.
REQ.3	Решението трябва да поддържа Multi-cloud решения и да позволява организациите да ползват облачно базирани услуги.
REQ.4	Решението трябва да разполага с централизиран Web базиран интерфейс за управление
REQ.5	Решението трябва да позволява защита на данните (бекъп) чрез прилагане на политики през потребителския интерфейс или основния интерфейс на защитаваните приложения
REQ.6	Решението трябва да позволява възстановяване на данни (restore) през потребителския интерфейс или основния интерфейс на защитаваните приложения
REQ.7	Решението трябва да позволява на администраторите на приложения да извършват операции по съхранение и възстановяване (backup / restore) през средствата на защитаваните приложения, като в същото време бекъп администраторите да наблюдават и контролират корпоративните политики (oversight and governance)
REQ.8	Решението трябва да поддържа SaaS базирано наблюдение и отчети, които позволяват да се наблюдават детайлно дейностите по защита на данните и дефинираните политики
REQ.9	Решението трябва да поддържа дедупликация и интеграция със специализирани масиви за съхранение на архивни данни (purpose build backup appliances)
REQ.10	Решението трябва да използва дедупликация с променлив размер на блоковете (variable-length data segments) за максимална ефективност
REQ.11	Решението трябва да позволява бързи и ефективни дневни пълни архиви (full backups), като намалява натоварването на процесора
REQ.12	Решението трябва да поддържа директен бекъп от приложението към специализираното бекъп устройство (Purpose build backup appliance). Този възможност трябва да е налична за всички типове бекъп, за да се намали натоварването на бекъп инфраструктурата
REQ.13	Решението трябва да поддържа следните типове приложение:
REQ.14	Kubernetes (with app-consistent backup of DB's).
REQ.15	Поддържани хипервайзори – минимум VMware и Hyper-V
REQ.16	Поддържани приложения: Microsoft SQL, Exchange, Active Directory, Oracle, SAP HANA
REQ.17	Windows, Linux, file systems.
REQ.18	Решението трябва да позволява защитата и възстановяването на данни от NAS ресурси.
REQ.19	Решението трябва да позволява стартиране на виртуална машина директно от бекъп сториджа.

REQ.20	Решението трябва да позволява управление на бекъпите директно от vCenter, чрез прилагане на политики по време на създаване на виртуалните машини, чрез използване на политики за архивирани.
REQ.21	Решението трябва да поддържа репликация на архивираните данни за DR възстановяване
REQ.22	Решението трябва да има интеграция с дискови масиви за съхранение на архиви и разпознава репликираните архиви на ниво дисков масив за DR възстановяване
REQ.23	Решението трябва да предлага криптиране на данните
REQ.24	Решението трябва да предоставя права на база на роли (role-based)
REQ.25	Решението трябва да предоставя REST API
REQ.26	Решението да бъде лицензирано за 6 процесора
REQ.27	Лицензите трябва да позволяват използването на всички типове агенти за операционни системи, бази данни и приложения, без ограничения в техния брой (ограничението на брой лицензирани процесори и/или капацитет)
REQ.28	Ако инсталацията на компонентите на софтуера изискват допълнителни софтуерни продукти като операционни системи, бази данни и др., то всички допълнителни лицензи трябва да бъдат включени в офертата. Поддръжката на тези допълнителни лицензи трябва да отговаря на поддръжката на бекъп софтуера.
REQ.29	Лицензите трябва да се доставят с минимум 3 години поддръжка.

2.3. Доставка на решение за предотвратяване на изтичане на данни от крайни точки със следните минимални технически изисквания:

Минимални технически изисквания	
REQ. 1.	Предложеното решение трябва да включва лицензи за 550 Windows-базирани крайни точки, 10 Linux-базирани крайни точки и 40 терминални сървъра. 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 групова 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 определни 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 сихронизиране 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 утройства -в локалната мрежа (споделени мрежови дялове) -в Интернет, минимално чрез email клиенти, приложения за споделяне на файлове, уеб браузъри, Instant Messaging платофрми, 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 притниране 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 анализираните 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 конфигурациятаи 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 файлови „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 месеца
REQ. 44.	Възможност за обновление на софтуера в периода на поддръжката до последна актуална версия на производителя.

2.4. Доставка на система посредник до интернет със следните минимални технически изисквания:

Минимални технически изискваня	
REQ.1	Да има възможност за инсталиране върху VMWare ESXi
REQ.2	Система за контрол и защита на потребителите при тяхната работа с WEB портали и Web приложения през Internet.
REQ.3	Да поддържа работа като HTTP, HTTPS, FTP и SOCKS прокси.
REQ.4	Да поддържа „прозрачен“ и proxy режим на работа.
REQ.5	Да поддържа SSL декриптиране.
REQ.6	Да поддържа филтриране на достъпа до URL адреси по категории и репутация на Web порталите.
REQ.7	Да има вградена DPI система за разпознаване на приложения.
REQ.8	Да разпознава WEB стрийминг на аудио и видео и да поддържа отделни трафични политики ограничаващи пропускателната лента както за всеки потребител, така и за достъпа до определена стрийминг услуга от всички потребители.
REQ.9	Да поддържа създаването на политики за филтриране на достъпа до Web приложения.
REQ.10	Да поддържа динамично сканиране и управление на достъпа до съдържанието в търсената от потребителя WEB страница: · Медия файлове · Изпълними файлове · Инсталатори · Документни формати · Проверка в архиви · Flash съдържание · MIME типове · P2P мета файлове
REQ.11	Да поддържа „деконструиране“ на WEB страниците до техните основни обекти и тяхното индивидуално сканиране.
REQ.12	Да поддържа разширена проверка на файлове за наличието на зловреден код: · Да използва система за откриване на файлове със зловреден код на базата на сигнатури. · Да използва система базирана на файлови „отпечатъци“ за откриване на полиморфни форми на зловреден код. Системата за сравняване на файлови отпечатъци трябва да използва „размита логика“ (fussy logic) за сравняване на близки/ подобни файлови отпечатъци. Системата трябва да поддържа напълно автоматично събиране на метаданни за всеки файл и изготвяне на уникални файлови отпечатъци за тях. · Да използва технологии за машинно самообучение на системата за класификация, на база статистически алгоритми анализиращи поведенческите атрибути на вече класифицирани файлове (класифицирани като „добри“ или като съдържащи зловреден код). Предлаганото решение трябва да може да се възползва от резултатите на статистическите анализи извършвани и за други клиенти, използващи решението на производителя. · Да притежава възможност за ретроспективни проверки – съхраняване историята на всички проверени файлове и извършване на нова

	класификация при получаване на нова информация (файлови сигнатури, отпечатъци и т.н).
REQ.13	Да поддържа създаването на политики за времеви и трафични ограничения на групи от потребители до определени категории WEB портали
REQ.14	Да поддържа сканиране на комуникациите, на L4 ниво, за установяване на зловреден софтуер, който се опитва да избегне комуникация през порт 80.
REQ.15	Да поддържа управление на файловият ъплоад с политики, на база репутацията и категорията на Web порталите към които се качват файлове.
REQ.16	Да позволява интеграция с външни DLP системи чрез ICAP протокол.
REQ.17	Да има възможност за добавяне на Web защита за потребители, които се намират извън мрежата на възложителя.
REQ.18	Да има вградена система за управление и наблюдение с WEB интерфейс: · Анализ и отстраняване на заплахите. · Управление на политиките за филтриране. · Трафични тенденции. · Използвани WEB апликации и трафичните им тенденции. · Детайлни доклади за WEB потребителите. · Посетените URL адреси и категории портали. · Анализи на опитите за използване на всички L4 портове с идентифициране на хостовете и потребителите. · Визуализиране на тенденции, проследяване и отстраняване на проблеми.
REQ.19	Да поддържа интеграция с Microsoft Active Directory за идентификация на потребители и групи и прилагане на политики върху тях.
REQ.20	Софтуера да има инсталирана и лицензирана, с постоянен лиценз, операционна система и база данни, които поддържат гореописаните функции.
REQ.21	Софтуера да е окомплектован със съответните лицензи и права за използване според условията на производителя за минимум 300 потребителя.
Гаранция и поддръжка:	
REQ.22	Срок на техническа поддържка – минимум 36 месеца.
REQ.23	Получаване на нови версии на софтуера - минимум 36 месеца.
REQ.24	Обновяване на дефиниции и сигнатури – минимум 36 месеца.

3. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО

3.1. Изисквания към изпълнението за точка 2.1са следните:

- Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя или официален негов представител за право на разпространение/доставка на предлаганите хардуерни продукти на територията на Република България 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;
- При невъзможност за отстраняване на настъпила повреда и/или несъответствие, следва да бъде осигурено оборотно оборудване, притежаващо характеристиките на доставеното устройство, включително нови алтернативни решения при запазване на пълната изисквана функционалност, до пълното отстраняване на повреда или несъответствие, като срока на гаранционно обслужване на оборудването в процес на поправяне, се удължава със срока, през който е траело отстраняването на повредата;
- 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.

3.2. Изискването към изпълнението на точки 2.2.,2.3 и 2.4 е следното:

Изпълнителят следва да осигури продуктите от лице, надлежно оторизирано от производителя на софтуерните продукти или официален негов представител за правото на разпространение/доставка на предлаганите софтуерни продукти на територията на Република България.

4. МЯСТО НА ИЗПЪЛНЕНИЕ

Мястото на изпълнение е сградата на Сметна палата на Република България, намираща се на адрес: гр. София, ул. „Екзарх Йосиф“ № 37.

5. 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 Възложителя/Бенефициера (МИДТ/СП) 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

[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 (МИДТ/СП), които са предмет на защита съгласно приложимото законодателство в областта.

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

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 (МИДТ/СП);

(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 (МИДТ/СП), 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 (МИДТ/СП) и на Изпълнителя извършват анализ и набелязват мерки за отстраняване на допуснатата нередност в определен срок.