Приложение № 2
към рамков договор № ПО-16-1466/16.11.2020 г.

Заявка
по рамков договор № ПО-16-1466 от 16.11.2020 г.

Позиция от ПГ-2024 г.:	*№ по ред от ПГ*	*1*
Описание на дейност/проект съгласно ПГ:	Системно администриране на ЦАИС ЕОП	
CPV код	*50324100*	
Изискване за достъп до класифицирана информация ДА/НЕ	*Да - за служителите, които ще изпълняват дейности по заявката на място в съответните центрове за данни, предоставени от Изпълнителна агенция „Инфраструктура на електронното управление“ (ИА ИЕУ)*	
Стойност: (*стойността следва да съответства на заложената в План-графика***) без ДДС**		*1 012 440,00 лв. без ДДС*
Срок за плащане: *(еднократно, на части, периодично или др.)*	*На части, както следва:* • *За периода от 01.01.2024 г. до 30.09.2024 г.: на тримесечие, след подписване от страните на приемо-предавателен протокол (ППП) по чл. 6 от договора, удостоверяващ приемане на извършените дейности по системно администриране на ЦАИС ЕОП за съответния тримесечен отчетен период ведно с доклад за извършените дейности през тримесечния период и фактура на стойност 233 640,00 лв. без ДДС за всяко тримесечие;* • *За периода 01.10.2024 г. – 30.11.2024 г.: след подписване от страните на приемо-предавателен протокол (ППП) по чл. 6 от договора, удостоверяващ приемане на извършените дейности по системно администриране на ЦАИС ЕОП за отчетния период ведно с доклад за извършените дейности през периода и фактура на стойност 155 760,00 лв. без ДДС за периода;* • *За периода 01.12.2024 г. – 31.01.2025 г.: след подписване от страните на приемо-предавателен протокол (ППП) по чл. 6 от договора, удостоверяващ приемане на извършените дейности по системно администриране на ЦАИС ЕОП за отчетния период ведно с доклад за извършените дейности през периода и*	

	фактура на стойност 155 760,00 лв. без ДДС за периода.
Плащане с акредитив ДА/НЕ	*НЕ*
Документи за плащане с акредитив	*Неприложимо*
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*Срок за изпълнение на услугата – от 01.01.2024 до 31.01.2025 г., включително*
Гаранционен срок:	*Неприложимо*
Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*	*На части, както следва:* • *За периода от 01.01.2024 г. до 30.09.2024 г.: На тримесечие, с подписване от страните на приемо-предавателен протокол (ППП) по чл. 6 от договора, удостоверяващ приемане на извършените дейности по системно администриране на ЦАИС ЕОП за съответния тримесечен отчетен период ведно с доклад за извършените дейности през тримесечния период;* • *За периода 01.10.2024 г. – 30.11.2024 г.: с подписване от страните на приемо-предавателен протокол (ППП) по чл. 6 от договора, удостоверяващ приемане на извършените дейности по системно администриране на ЦАИС ЕОП за отчетния период ведно с доклад за извършените дейности през периода;* • *За периода 01.12.2024 г. – 31.01.2025 г.: след подписване от страните на приемо-предавателен протокол (ППП) по чл. 6 от договора, удостоверяващ приемане на извършените дейности по системно администриране на ЦАИС ЕОП за отчетния период ведно с доклад за извършените дейности през периода.*
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:	*Подпис:*

Ръководител на проект/дейност по заявката (напр: представител на дирекцията – Заявител):		*Подпис:*
ЗАЯВКАТА е ОДОБРЕНА ОТ:		
ВЪЗЛОЖИТЕЛЯ:		*Подпис:*
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:		
Координатор от „Информационно обслужване“ АД по заявката		*Подпис:*
Ръководител на проект/дейност по заявката от „Информационно обслужване“ АД		*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

Системно администриране на Централизирана автоматизирана информационна система „Електронни обществени поръчки“ (продукционна, резервна, тестови подсистеми и Call Center)

1 Въведение

Експлоатацията на Централизираната автоматизирана информационна система „Електронни обществени поръчки“ (ЦАИС ЕОП или Системата) изисква полагане на грижи и усилия за осигуряване на непрекъснатост (24x7) и висока наличност на ИКТ услугите, които осигуряват бизнес процесите, реализирани в ЦАИС ЕОП. Същевременно е необходимо и постоянно проактивно наблюдение и администриране на инфраструктурата и комуникационната среда на ЦАИС ЕОП. В настоящото изложение са представени описание на Системата и обхватът на дейностите по системното ѝ администриране. Посочени са конкретни изисквания към начина на предоставяне на услугата „системно администриране на ЦАИС ЕОП“.

За техническите дейности, описани по-долу, са използвани политики, процедури и указания на The European Union Agency for Cybersecurity (ENISA), The National Institute of Standards and Technology (NIST), SANS Institute и други източници.

2 Описание на ЦАИС ЕОП

Оборудването на ЦАИС ЕОП е разположено в два центъра за данни – ЦД1 и ЦД2. В ЦД1 са реализирани продукционната (експлоатационната) и публичната тестова среди, а в ЦД2 – резервната среда на Системата и тестовата среда, използвана при надграждания ѝ. Оборудването на Център за обслужване на клиенти (Call Center) е разположено в помещения на Агенцията по обществени поръчки.

В режим 24x7 се администрират всички среди и системи, а именно:

- продукционната среда;
- резервната среда;
- публичната тестова система;
- тестовата система DEVTEST;
- Call Center.

Съгласно Закона за защита на класифицираната информация, всеки член на екипа, осъществяващ дейности по системно администриране на ЦАИС ЕОП на място в съответните центрове за данни, предоставени от ИА ИЕУ, е задължително да разполага с разрешение за достъп до класифицирана информация до ниво „СЕКРЕТНО“.

Компонентите, изграждащи ЦАИС ЕОП, включват:

№	Компонент	Брой
1.	Физически сървъри	14
2.	Виртуални машини	84
3.	Комуникационни устройства	24
4.	Дискови масиви/устройства за съхранение на данни	5
5.	Сървърни операционни системи	4
6.	Desktop операционни системи	1

№	Компонент	Брой
7.	СУБД	2
8.	Бази данни	21
9.	Виртуализационни среди	1
10.	SMTP сървъри	2
11.	Софтуерни системи за наблюдение	3
12.	Други – софтуер за архивиране и възстановяване, софтуер за управление достъпа на привилегировани потребители, услуга за двуфакторна автентикация на потребители и др.	
13.	Център за данни	2
14.	Подсистема (среда)	5

Забележки:

Детайлна информация относно хардуерните и софтуерните компоненти на ЦАИС ЕОП може да бъде намерена в описанието на архитектурата на Системата, в два файла - System Design.docx (Приложение № 1) и DEVTEST_aop1.docx (Приложение № 2), които се предоставят по електронна поща на ръководителя на проекта от страна на Изпълнителя преди стартиране на изпълнението на заявката и се актуализират по време на изпълнението на проекта.

За целите на настоящия документ, за компоненти на ЦАИС ЕОП се считат и специализираните хардуерни и софтуерни компоненти, необходими и използвани за системното администриране на ЦАИС ЕОП.

3 Дейности в обхвата на заявката

3.1 Администриране на сървърните системи

3.1.1 Непрекъснат (24x7) проактивен мониторинг от страна на Изпълнителя на наличността, работоспособността и достъпността на сървърните системи (включително виртуалните устройства, включени в архитектурата) на ЦАИС ЕОП чрез система за наблюдение, осигурена и поддържана от Изпълнителя, външна за средите на ЦАИС ЕОП;

3.1.2 Системно администриране на сървърните системи в продукционната, резервната и тестовите подсистеми.

Системно администриране на Windows базирани системи и на Windows операционни системи, включващо:

a) Конфигуриране на основни и базови услуги;
b) Конфигуриране на планирани задачи (Scheduled tasks);
c) При необходимост, оказване на съдействие при инсталиране и конфигуриране на 3rd party софтуер;
d) Анализ и оценка за необходимостта от осъвременяване на версиите на софтуера, извършване на осъвременяването.

Системно администриране на Linux операционни системи, включващо:

a) Конфигуриране на основни и базови услуги;
b) Конфигуриране на планирани задачи (Crontab jobs);
c) При необходимост, оказване на съдействие при инсталиране и конфигуриране на 3rd party софтуер;
d) Анализ и оценка за необходимостта от осъвременяване на версиите на софтуера, извършване на осъвременяването.

Системно администриране на VMware софтуер за виртуализация, включващо:

a) Обновяване на софтуера до актуална версия;
b) Анализ на необходимостта от прилагането на обновления и поправки, издадени от производителя на софтуера;
c) Проактивен мониторинг на разпределението на ресурсите на виртуализационните платформи;
d) Имплементиране на промени във виртуалните среди с цел използване на допълнителни инфраструктурни ресурси - дискови масиви, мрежова свързаност и други;
e) Администриране и конфигуриране на достъпа до виртуалните инфраструктури;
f) Конфигуриране на права за достъп до виртуалните машини.

Системно администриране на активна директория (MS Active Directory), включващо:

a) Управление на Active Directory услугата;
b) Управление на AD Site Topology;
c) Управление на домейни;
d) Управление на Operations Master;
e) Управление на схемата Active Directory;
f) Управление на репликацията между Domain Controllers (DC).

Системно администриране на DNS услуга, включващо:

a) Управление на DNS сървъри;
b) Управление на DNS зони;
c) Управление на състоянието на DNS услугата;
d) Управление на репликацията между DNS сървърите;
e) Управление на публичния домейн eop.bg.

Системно администриране на специализирани софтуери за управление на обновленията, включващо:

a) Управление на WSUS (Windows Server Update Services) сървъри;
b) Управление на Apt-Cacher NG сървъри;
c) Управление на състоянието на кръпки (patches) по сигурността чрез WSUS сървърите;
d) Управление на пакетите за обновление на Linux машините чрез Apt-Cacher NG сървърите.

Системно администриране на архивирането, включващо:

a) Настройване и управление на решението за архивиране и възстановяване – администриране на специализирания софтуер за архивиране и възстановяване Veeam;
b) Управление на резервирането на данни по предварително изготвена архивна схема (Backup plan) спрямо нуждите на сървърните приложения;
c) Обновяване на архивната схема при необходимост;
d) Управление на архивните задачи;
e) Създаване на нови архивни задачи чрез специализирания софтуер и/или средствата за архивиране, вградени в операционните системи;
f) Наблюдение на процесите на архивиране;
g) Разрешаване на проблеми, свързани с архивирането на Системата;
h) Наблюдение на състоянието на архивите на операционните системи;

i) Наблюдение на състоянието на архивите на основните приложения в ИКТ инфраструктурата;
j) Наблюдение на състоянието на архивите на 3rd party приложения в ИКТ инфраструктурата;
k) Управление на процеса по архивиране на информацията - следене за успешното протичане на архивирането на ЦАИС ЕОП;
l) Извършване на всеки 3 месеца на тестови възстановявания от архиви на виртуални машини и ежемесечно от архиви на бази данни с цел проверка на тяхното качество, консистентност и цялост;
m) Системно администриране на системите за съхранение на данни, включващо локални дискови масиви, споделени дискови масиви, дейта домейни и SAN инфраструктурата.

Системно администриране на SAN инфраструктурата, включващо:
a) Системно администриране на дисковите масиви за съхранение на данни;
b) Системно администриране на виртуализираното дисково пространство.

Системно администриране на кръпки (patches) в сигурността, включващо:
a) Тестване на кръпки по сигурността за различните видове приложения и операционни системи;
b) Инсталиране на одобрените кръпки за различните видове приложения и операционни системи;
c) Инсталиране на одобрените кръпки на версии на 3rd party приложения.

Системно администриране, включващо минимум обновяване на версиите на софтуера WordPress и на плъгините, използвани за изграждане Портала за обществени поръчки, и администриране на web сървъра и страницата/подстраниците на портала. В обхвата на администрирането се включва и тестовият сайт с адрес https://www-test.eop.bg.

3.1.3 Допълнителни технически дейности по сървърните системи:
a) Гарантиране на еталонните параметри на процесорно натоварване, използване на RAM памет, свободно дисково пространство, наличие и скорост на мрежова свързаност в продукционната, резервната и тестовите подсистеми;
b) При необходимост - мигриране на внедрените приложения и програмни продукти;
c) Системно администриране на сървърните системи, обслужващи Call Center;
d) Координиране на действията, необходими за разрешаване на проблеми, свързани със сървърните системи на ЦАИС ЕОП, с АОП и външни доставчици на услуги;
e) Анализ на рисковете и преценка за необходимостта от инсталиране на нови компоненти на базовия системен софтуер (patches, updates, Services Packs, нови версии на софтуер/firmware, изтичане на поддръжка и други);
f) Преди извършване на инсталация да се правят резервни копия на софтуера, файловете и базите данни и да се разработи roll back план в случай на неуспешна инсталация;
g) Обновяване на цифрови сървърни сертификати;
h) Настройване, поддържане на нормалната работа на SMTP сървър – Postfix, обслужващ ЦАИС ЕОП, и извършване, по заявка на АОП, на проверки в логовете на сървъра за изпратени електронни съобщения.

3.2 **Администриране на системите за управление на бази данни (СУБД)**

3.2.1 Непрекъснат проактивен мониторинг на работоспособността на СУБД в продукционната, резервната и тестовите подсистеми чрез система за наблюдение, осигурена и поддържана от Изпълнителя, външна за средите на ЦАИС ЕОП;

3.2.2 Системно администриране на сървърите, обслужващи СУБД, на специализиран приложен софтуер на сървърите и на информационните масиви за съхранение на бази данни, включващо:

a) Ежедневен контрол на параметрите и работоспособността на СУБД;
b) Системно администриране на роли в приложните сървъри, свързани с информационните масиви за съхранение на данни/бази данни;
c) Системно администриране на сървърни приложения, в частта им, взаимодействаща с информационните масиви за съхранение на данни/бази данни;
d) Наблюдение и осигуряване на нормалното функциониране на специализираните приложни системи;
e) Отчитане, коригиране и докладване за често повтарящи се грешки;
f) Проучване на възможните грешки и последствия за информационните масиви за съхранение на данни/базите данни при обновяване на версията и възможностите за оптимизация при преминаване към по-нова версия;
g) Проверки и профилактики на продукционната, резервната и тестовите системи: всекидневни, седмични и месечни, в съответствие с преценена от Изпълнителя необходимост;
h) Архивиране и предоставяне на статистическите файлове;
i) Промени на системни настройки;
j) Управление и справки от информационните масиви за съхранение на данни/базите данни за потребителите;
k) Обновяване на информационните масиви за съхранение на данни/базите данни, като всички обновления се прилагат и тестват на предварително изградена тестова среда;
l) Ежемесечно извършване на тестови възстановявания от архиви на базите данни с цел проверка на тяхното качество, консистентност и цялост, при възможност в присъствието на експерт/и от АОП;
m) Наблюдение на поведението на СУБД чрез логовете.

3.3 **Администриране на комуникационните системи (КС)**

3.3.1 Непрекъснат проактивен мониторинг на работоспособността на комуникационните системи (включително виртуални) и комуникационните канали и връзки в продукционната, резервната и тестовите подсистеми чрез система, осигурена и поддържана от Изпълнителя, външна за средите на ЦАИС ЕОП. Непрекъснат мониторинг на свързаността на ЦАИС ЕОП с доставчиците на квалифицирани електронни удостоверителни услуги, със средата за междурегистров обмен на информация Regix;

3.3.2 Системно администриране на комуникационните системи и преносната среда (LAN и WAN, специализирани устройства за разпределяне на мрежовия трафик, Firewalls, интернет свързаност, комуникационни канали от и към Единната електронна съобщителна мрежа (ЕЕСМ) на държавната администрация), включващо:

a) Промени в конфигурацията и настройките на комуникационните канали/връзки и КС, когато се налага;
b) Архивиране на конфигурациите на активното мрежово оборудване и поддържане на история на конфигурациите;

c) Измерване и анализ на параметрите на трафика и изготвяне на предложения за оптимизации;
d) Управление на връзките за интернет свързаност на ЦАИС ЕОП;
e) Управление на връзките между центровете за обработка на данни на ЦАИС ЕОП;
f) Управление на LAN на ЦАИС ЕОП;
g) Следене на логовете (logs) на комуникационните системи и канали;
h) Актуализиране на КС в продукционната, резервната и тестовите среди.

3.4 **Управление на логовете (Logs)**

3.4.1 Управление на системни логове, включително логовете на виртуализационния софтуер, операционните системи, СУБД, КС, помощни софтуери и др. - оценка след съгласуване с АОП кои имат стойност в дългосрочен план и според законови изисквания не трябва да бъдат изтривани;

3.4.2 Периодично архивиране/изтриване на неполезни логове след съгласуване с АОП;

3.4.3 Анализ, включително корелативен, на одитните събития, записани в логовете, с цел идентифициране на проблеми и зависимости и установяване на тенденции;

3.4.4 Наблюдение за грешки и предупреждения в Event Logs на Windows базирани сървъри;

3.4.5 Наблюдение за предупреждения и грешки в системни логове (syslog, messages, deamon и други) за Linux базирани сървъри;

3.4.6 Наблюдение на състоянието на Scheduled tasks;

3.4.7 Наблюдение на състоянието на Crontab jobs;

3.4.8 Наблюдение на логовете на комуникационната среда.

3.5 **Наблюдение на състоянието на хардуера**

3.5.1 Наблюдение на състоянието на хардуера чрез специализиран централизиран софтуер;

3.5.2 Наблюдение на състоянието на хардуера чрез специализиран софтуер, предоставен от производителя на хардуера;

3.5.3 При откриване на дефект Изпълнителят следва да уведоми АОП и да предостави детайли за целите на изготвянето на заявка към изпълнителя на хардуерната поддръжка в случаите на дефектирало оборудване с изтекла гаранционна хардуерна поддръжка.

3.6 **Информационна сигурност**

3.6.1 Общо изискване: Всички дейности по системното администриране на ЦАИС ЕОП трябва да поддържат ниски нива на информационни рискове и да се гарантира конфиденциалността, интегритета и достъпността на трансфериранатa, обработваната и съхраняваната информация в ЦАИС ЕОП, включително Call Center;

3.6.2 Изпълнителят се задължава да спазва относимите разпоредби на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (в приложимите случаи), като предприема всички необходими действия и мерки за защита на личните данни, до които имат достъп при изпълнение на настоящата заявка;

3.6.3 Сканирания за техническите уязвимости и прилагане на мерки за отстраняване на откритите слабости:

Изпълнителят е длъжен да сканира поне веднъж на три месеца за технически уязвимости всички работещи в ЦАИС ЕОП информационни системи - мрежови,

сървърни и интернет сайтовете. Тестовете за технически уязвимости трябва да бъдат извършвани чрез автоматизирани инструменти (ползващи база данни от Network Vulnerability Tests (NVTs)) и чрез прилагане на експертни неавтоматизирани методи - ръчни проверки. Процесът на тестване трябва да обхваща публично достъпните и локалните информационни ресурси на ЦАИС ЕОП и проверка за наличие на Common Vulnerabilities and Exposures (CVE), регистрирани в глобалните бази данни. Необходимо е всяко открито несъответствие да се анализира и оценява чрез Common Vulnerability Scoring System (CVSS), която дава информация за характеристиките на уязвимостите и формира оценки на критичността им;

3.6.4 Изпълнителят трябва да анализира всички системи за наличие на зловреден софтуер и да преконфигурира, надстройва, преинсталира или деинсталира приложения и/или операционни системи. Поне веднъж на всеки три месеца трябва да се извършват следните дейности:

a) Сканиране за технически уязвимости и прилагане на мерки за отстраняване на откритите несъответствия за всички публично достъпни ИКТ услуги на ЦАИС ЕОП, включително интернет сайтовете;
b) Сканиране за технически уязвимости и прилагане на мерки за отстраняване на откритите несъответствия за всички ИКТ ресурси в локалните мрежи на ЦАИС ЕОП;
c) Преглед на сървърните системи за наличие на зловреден софтуер;
d) Анализиране за компютърни вируси;
e) Анализиране за известни RootKits – механизми и техники, чрез които зловредни програми, включително компютърни вируси, шпионски програми и троянски коне, се опитват да се скрият от антивирусни програми и други приложения за сигурност;
f) Анализиране за участие на сървърните системи в botnets;
g) Анализиране за инсталиран софтуер без знанието на системните администратори, който събира лична информация (spyware), в това число софтуер за събиране на пароли (keylogger);
h) Анализиране за софтуер, който управлява рекламни съобщения (adware);
i) Анализиране на интернет сайтовете на АОП за риск от атаки (DoS, DDoS, SQL injection).

3.7 Администриране на допълнителни софтуерни компоненти и услуги

3.7.1 Администриране на софтуерните средства, използвани за поддържане на инфраструктурата:

a) Софтуерни системи за наблюдение – настройване на софтуерните системи, дефиниране на наблюдавани обекти, праговете за уведомления, праговете за критични събития, e-mail адреси за изпращане на автоматични съобщения;
b) Софтуерни системи за обновяване на сървърни операционни системи и за архивиране на конфигурации – преглеждане на ъпдейти и настройване на време за прилагането им, настройване на периодично архивиране на конфигурационни файлове;
c) Сървъри за сканиране за уязвимости на публичните и локалните ресурси.

3.7.2 Администриране на софтуерни средства за управление на потребители:

a) Услуга за двуфактурна автентикация на потребители (SafeNet Trusted Access) – дефиниране на политики за управление на потребителите, управление на потребители и др.;

b) Софтуерна система за управление достъпа на привилегировани потребители (PAM - Privilege Access Management) – дефиниране на политики за управление на потребителите, настройване на потребители, дефиниране на обекти за привилегирован достъп, дефиниране на параметри за запис, съхранение и унищожаване на видеозаписи и др.;
c) Настройване на отдалечена VPN свързаност за служители на Изпълнителя и на Агенцията по обществени поръчки.

3.7.3 Администриране на софтуерни средства, използвани в Call Center:
a) Приложение за софтуерна телефонна централа – настройване на системата, потребители, телефонни номера, автоматични гласови съобщения, съхранение на аудиозаписи от работата на Call Center и др.;
b) Приложение за управление на проекти (Redmine) – настройване на потребители, интеграция на приложението със софтуерната телефонна централа, интеграция на приложението с пощенския сървър на АОП.;
c) Администриране на приложението за софтуерен телефон и операторските работни станции.

3.7.4 Поддържане на наличността и нормалното функциониране в ЦАИС ЕОП на външни услуги:
a) Осигуряване наличието на външна квалифицирана услуга за удостоверяване на време, използвана в ЦАИС ЕОП – наблюдение, конфигуриране при необходимост, комуникация с основния и резервния доставчик на услугата;
b) Осигуряване проверката за валидност на квалифицирани електронни подписи чрез връзка с всички доставчици на квалифицирани услуги, включени в Националният доверителен списък, поддържан от Комисията за регулиране на съобщенията;
c) Осигуряване на нормална свързаност с външни информационни системи – TED, e-Certis, Търговски регистър, Регистър БУЛСТАТ, Електронни услуги на НАП, Регистър на КЗК, както и със средата за междурегистров обмен на данни (Regix);
d) Ако в срока на изпълнение на настоящата заявка бъде реализирана и внедрена интеграция на ЦАИС ЕОП с други външни информационни системи (например Информационна система за бюджетен контрол, система за електронна идентичност, система за електронна идентификация и др.), поддържането на нормална свързаност с тези системи също попада в обхвата на заявката.

3.7.5 Други:
a) Администриране на информационни ресурси на ЦАИС ЕОП, създавани или променяни при надграждания на Системата (с изключение на MATOMO);
b) Възстановяване след срив на нормалната информационна и комуникационна инфраструктура на ЦАИС ЕОП;
c) Поддържане на единно точно време на системите в съответствие с изискванията на чл. 46 от Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги;
d) Предприемане на мерки за отстраняване на открити несъответствия и уязвимости за всички публично достъпни услуги и за всички ИКТ ресурси в локалните мрежи на ЦАИС ЕОП в резултат на одити, проверки и тестове, извършени от трета страна (независима от АОП и Изпълнителя);
e) Мигриране на подсистеми на ЦАИС ЕОП в нови локации при необходимост;
f) Дейности по включване на ЦАИС ЕОП в Държавния хибриден частен облак (ДХЧО), ако в рамките на срока на изпълнение на настоящата заявка Възложителят предприеме такова включване.

3.8 **Разрешаване на инциденти и проблеми**

Разрешаването на инциденти/проблеми, свързани със състоянието и работоспособността на комуникационната и информационната инфраструктура и ресурси на ЦАИС ЕОП, архивирането и информационната сигурност на Системата, също е в обхвата на дейностите по системно администриране, предмет на настоящата заявка.

Задължение на Изпълнителя е и уведомяването на АОП чрез система за управление на заявки (СУЗ), осигурена и поддържана от Изпълнителя, външна за средите на ЦАИС ЕОП. Уведомяването се извършва при нарушаване на наличността, работоспособността или достъпността на компонент на комуникационната и/или информационната инфраструктура на ЦАИС ЕОП. В случай на събитие, за което експерт на Изпълнителя, прецени, че е инцидент, моментът на уведомяване чрез системата се счита за начало на срока за реакция и отстраняване на проблема. Ако информация за събитието е постъпила по няколко комуникационни канала (и по телефон или електронна поща), за начало на срока за реакция и отстраняване на проблема се счита най-ранното уведомяване.

Инциденти/проблеми трябва да могат да се съобщават на Изпълнителя от служители на АОП по телефон, по ел. поща и чрез СУЗ. Комуникацията се осъществява на български език.

Инцидентите и проблемите се разделят на две групи в зависимост от приоритета им:

- **Приоритет 1**: вследствие от инцидента/проблема са налице прекъсвания в работата на Системата, които се отразяват на широк кръг потребители; наблюдават се пропадания или нарушения в комуникациите; важни функции на редовната дейност не могат да бъдат обслужени или реализирани. Инцидентът/проблемът изисква незабавно внимание, за да се предотврати влошаването му и засягането на критични дейности и компоненти.
- **Приоритет 2**: инцидентът/проблемът не засяга основните функционалности на Системата, т.е. няма бизнес риск. Засегнати са ефективността и/или скоростта на изпълнение.

Приоритетите на инцидентите/проблемите се определят от Възложителя в зависимост от влиянието им върху работата на Системата. За задачи с Приоритет 1 следва да бъдат считани задачите, дефинирани в СУЗ с приоритети „висок“ и „критичен“.

Времето за локализация, диагностика на инцидента/проблема и възстановяване на нормалната работа на Системата, считано от момента на уведомяването за инцидента/проблема е, както следва:

- при инцидент/проблем от Приоритет 1 - не повече от 4 часа;
- при инцидент/проблем от Приоритет 2 - не повече от 72 часа.

Дефинират се три нива на ескалация на инцидентите/проблемите:

1-во ниво – служители от Call Center, експерти от АОП – установяват, приемат, систематизират и съобщават на 2-ро ниво за инцидента/проблема и евентуално предприети мерки.

2-ро ниво – екип на Изпълнителя за системното администриране на ЦАИС ЕОП – разглежда, анализира и отстранява всички възникнали инциденти/проблеми, попадащи в обхвата на настоящата заявка.

3-то ниво – мениджърски екип на Изпълнителя и представители на трети страни – намесва се, когато даден инцидент/проблем не може да бъде разрешен на 2-ро ниво. При необходимост от ескалация към трето ниво ръководителите на дейностите по настоящата заявка от страна на Възложителя и Изпълнителя трябва да бъдат уведомени незабавно. Ако се налага, те ескалират инцидента/проблема до ръководителите на

Възложителя и Изпълнителя, които може да отнесат проблема до представителите на трети страни, имащи отношение към поддръжката на ЦАИС ЕОП (напр. представители на Изпълнителна агенция „Инфраструктура на електронното управление“, представители на доставчици на удостоверителни услуги и др.). При необходимост се стартира процедурата за действия при непланирано прекъсване на ЦАИС ЕОП.

Екипът на системните администратори следва да оказва съдействие на екипа, извършващ следгаранционната софтуерна поддръжка на Системата, при изпълнение на процедурата за действия при непланирано прекъсване на ЦАИС ЕОП, както и при необходимост от актуализиране на същата.

3.9 Други технически дейности в обхвата на заявката

3.9.1 Управление на потребителите – управление на вградените акаунти, управление на акаунтите за служители, имащи отношение към системното администриране и поддръжката на ЦАИС ЕОП, включително служители на АОП - създаване на нови, промяна/изтриване на съществуващи, обновяване на пароли (в съответствие с политиката за сигурност, при необходимост, при искане от страна на Възложителя), инвентаризация на акаунтите;

3.9.2 Дейностите по системно администриране следва да се извършват само с персонализирани акаунти, освен в случаите когато това не е възможно;

3.9.3 Възложителят е длъжен да предостави на Изпълнителя пълен актуален списък на потребителите с администраторски права преди стартиране на изпълнението дейностите по заявката;

3.9.4 До 5 (пет) работни дни от направено писмено искане от страна на Възложителя, Изпълнителят е длъжен да предостави на Възложителя пълен актуален списък на потребителите с администраторски права;

3.9.5 Не по-рано от 10 (десет) и не по-късно от 5 (пет) работни дни преди изтичане на срока на изпълнение на настоящата заявка, Изпълнителят е длъжен да предостави на Възложителя пълен актуален списък на потребителите с администраторски права;

3.9.6 Списъците по предходните точки трябва да включват акаунти за операционните системи, за всякакъв специализиран и управляващ софтуер, за виртуализационни среди и виртуални устройства, за достъп до физически устройства, канали за връзка и др., т. е. всички акаунти, необходими за администрирането на ЦАИС ЕОП, страницата на АОП, комуникационните канали, системата за наблюдение на ЦАИС ЕОП, Call Center. За вградените администраторски акаунти се посочват техните пароли. Списъкът се предава в криптиран вид на лице/лица, определени от ВЪЗЛОЖИТЕЛЯ;

3.9.7 При необходимост провеждане на техническа профилактика на оборудването на ЦАИС ЕОП в рамките на срока на настоящата заявка с цел намаляване на риска от инциденти, предизвикани от технически повреди;

3.9.8 Оказване на експертна помощ на служители на АОП при необходимост;

3.9.9 Съдействие при одити и проверки, извършвани от външни организации.

3.10 Политики и процедури, необходими за осигуряване на наличността, достъпността, работоспособността и сигурността на ЦАИС ЕОП

Изпълнителят трябва да прилага минимум следните актуални политики и процедури:

a) Information Security Policy

b) Change Management Practice, включваща създаване и поддържане на актуална техническа документация с поддържане на история на версиите и съответните промени;
c) Incident Response Policy.

4 Общи изисквания

Системното администриране на ЦАИС ЕОП следва да се извършва отдалечено чрез VPN с изключение на случаите, при които характерът на дейността и инцидентът/проблемът не позволяват това. Администрирането на Системата следва да се извършва през PAM.

Компонентите на техническата документация следва да се поддържат актуални с история на версиите и да се съхраняват на споделено пространство с осигурен постоянен достъп за експертите на АОП.

Дейностите по системно администриране по възможност трябва да се планират и всички лица, използващи/поддържащи засегнатите ресурси, следва да бъдат уведомявани не по-малко от 3 дни преди извършване на дейността.

Дейностите по системно администриране по възможност трябва да се извършват в периоди с минимално натоварване на съответните ресурси. Преди инсталиране в оперативно действащата Система на нови софтуерни и хардуерни компоненти те трябва да се тестват в тестова среда максимално близка до реалните работни условия.

При разрешаването на инциденти/проблеми, попадащи в обхвата на настоящата заявка, експертите на Изпълнителя трябва да съгласуват своите действия с експертите, осъществяващи следгаранционната поддръжка на ЦАИС ЕОП и с експертите, реализиращи надграждания на Системата и тяхната гаранционна поддръжка. При инциденти/проблеми, произтичащи от състоянието на хардуерното оборудване, експертите на Изпълнителя трябва да съгласуват своите действия с фирмите, осъществяващи хардуерната поддръжка на ЦАИС ЕОП и да оказват съдействие на техните експерти. При всички случаи на осъществена комуникация с експерти на други фирми Изпълнителят трябва да уведомява ръководителя на настоящата заявка от страна на АОП.

При разрешаване на инциденти/проблеми, произтичащи от състоянието на физическата среда, в която е разположено оборудването на Системата, и/или от състоянието на Единната електронна съобщителна мрежа, експертите на Изпълнителя трябва да уведомяват за инцидента/проблема ръководителя на настоящата заявка от страна на АОП. Той координира взаимодействието между Изпълнителя и ИА ИЕУ, така че да не се нарушават клаузите на подписаното между АОП и ИА ИЕУ споразумение за предоставяне на услугата „колокация“ по отношение на оборудването на ЦАИС ЕОП.

5 Начин на отчитане на изпълнението на дейностите по системно администриране на ЦАИС ЕОП

5.1 Отчитането на изпълнението се извършва за всеки отчетен период, с писмен доклад за извършените през периода дейности. Докладът се предоставя в срок до 10-то число на месеца, следващ отчетния период. Той трябва да съдържа най-малко следната информация:

5.1.1. Пълно описание на извършените дейности, вкл.:
a) Дата/период на извършване на дейността;
b) Засегната среда;
c) Засегнато устройство/функционален модул;
d) Тип събитие;
e) Причина за извършване на действията;

f) Описание на действията;
g) Помощен файл, съдържащ важна относима информация за действията (напр. история на използвани команди, архив на състояние на конфигурационен файл и др.);
h) Резултат от действията;
i) Лице/а, извършило/и действията.

5.1.2. Резултати от сканиранията за уязвимости;

5.1.3. Предложение за конкретни действия и мерки за постигане и поддържане на ниски нива на информационните рискове и индикативни срокове за тяхното изпълнение;

5.1.4. Таблица със стойности за всеки месец поотделно на параметри на информационните и комуникационните ресурси, имащи отношение към състоянието на ЦАИС ЕОП (натоварване на основните виртуални сървъри – web, приложни и за бази данни, заетост на дисковото пространство, големина на базите данни).

5.2 В срок до 10 (десет) дни от представянето му, Възложителят преглежда доклада и при необходимост писмено изисква от Изпълнителя да го коригира и/или допълни в срок до 5 (пет) работни дни. Приемането на доклада се удостоверява с подписването от страните на приемо-предавателен протокол по чл. 6 от договора;

5.3 По изключение (напр. при срив, непланирани спирания на ЦАИС ЕОП или други извънредни ситуации) и след писмено искане, вкл. чрез електронна поща, от страна на Възложителя, Изпълнителят следва в срок до 2 (два) работни дни след искането да предостави извънреден писмен доклад за състоянието на ЦАИС ЕОП, включващ изрично поискана информация;

5.4 Докладите се предоставят в електронен вид към приемо-предавателния протокол по чл. 6 за съответния отчетен период, позволяващ пълнотекстово търсене и копиране на части от съдържанието му, като съставящите ги файлове трябва да бъдат подписани от съответните упълномощени лица с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис;

5.5 В срок от 15 (петнадесет) календарни дни от началото на изпълнение на заявката Изпълнителят трябва да предостави на АОП актуализирани процедурите по т. 3.10, които прилага. Матриците на отговорностите, съдържащи се в тях, следва да бъдат предоставени на Възложителя и при промени на служителите на Изпълнителя, заети със системното администриране на ЦАИС ЕОП.