

УТВЪРДИЛ:

**ПРОФ. Д-Р АНЕЛИЯ КЛИСАРОВА
МИНИСТЪР НА
ОБРАЗОВАНИЕТО И НАУКАТА**

ДОКУМЕНТАЦИЯ

ЗА ВЪЗЛАГАНЕ НА ОБЩЕСТВЕНА ПОРЪЧКА

ЧРЕЗ ПУБЛИЧНА ПОКАНА С ПРЕДМЕТ:

**„Поддръжка, системно и техническо обслужване на сървъри,
прилежащо оборудване и информационни системи на МОН за срок от
12 месеца“.**

Съдържание на документацията:

I. Техническо задание, определящо предмета на поръчката, цел на предмета на поръчката, обхват на дейностите за реализация на поръчката, място и срок на изпълнението.

II. Критерий за оценка.

III. Прогнозна стойност за извършване на услугата.

IV. Срок за изпълнение.

V. Изисквания към участниците.

I. Техническо задание, определящо предмета на поръчката, цели на предмета на поръчката, обхват на дейностите за реализация на поръчката, време и място на изпълнението

1. Цел на поръчката

Настоящата поръчка има за цел осигуряването на нормалното функциониране на ИТ системите в Министерството на образованието и науката (МОН) изпълнението на работните процеси в него. Тези процеси се подпомагат от информационни системи, които предоставят определени услуги на МОН. Целта на поръчката е да се осигури непрекъснатата поддръжка и съответни гаранции за непрекъснатост на операциите, информационна сигурност и защита на данните на информационните системи.

2. Място на извършване на услугата

Местонахождението на точките, в които следва да се осъществи посочената услуга е както следва:

- Централна сграда на МОН – София, Дондуков 2А
- Сграда на НАЦИД – София, бул. “Д-р. Г. М. Димитров” 52 А
- ЦИОО – София, ул. Атанас Далчев 8
- Сграда на МОН (5ти блок) – София, Цариградско шосе 125
- Инспекторат на МОН – София, ул. Антим I, №17
- Дирекция ККР на МОН – София, Граф Игнатиев 15

3. Обща информация

Настоящото техническо задание съдържа:

- Описание на изнесените ИТ услуги - цели, обхват, дейности;
- Детайлни изисквания към функционалните и техническите параметри на ИТ услугите;
- Специфични изисквания към начина на предоставянето на ИТ услугите;
- Специфични изисквания за гарантирани параметри на обслужването;

4. Администриране, поддръжане и развитие на информационни системи и база данни

4.1. Цел на услугата

Целта на услугата е осигуряването на администриране и поддръжане на информационните системи на МОН (вкл. АИС за работа с класифицирана информация) и включва обслужване на следните елементи на ИТ инфраструктурата:

- **Системен и общ приложен софтуер;**
- **Специализиран приложен софтуер;**
- **Бази от данни;**
- **Хардуер;**
- **Комуникационно оборудване;**

4.2. Обхват на услугата

Настоящата услуга се отнася за системите разположени в сървърните помещения в описаните в т. 2 локации. Услугата не обхваща поддръжката на телефонните системи и специализиран софтуер, разработен за нуждите на МОН. Информационните системи, които подлежат на обслужване, са описани в Приложение № 2А.

4.3. Тип и управление на услугата

Услугата е регулярна т.е. тя се изпълнява непрекъснато през годината, без задължение за, но с право за подаване на заявки от ВЪЗЛОЖИТЕЛЯ.

4.4. Дейности по предоставянето на услугата

4.4.1. По отношение на сървърите ИЗПЪЛНИТЕЛЯТ следва да осигури следните дейности:

4.4.1.1. Ежедневен мониторинг на Windows базирани системи

- Наблюдение на наличността и работоспособността на операционната система;
- Наблюдение на състоянието на основните услуги на операционната система (services);
- Наблюдение на натоварването на процесорите;
- Наблюдение на количеството заета оперативна памет;
- Наблюдение на заетото (свободно) дисково пространство;

- Наблюдение на натовареността на дисковата подсистема;
- Наблюдение на натоварването на мрежовите интерфейси;
- Анализ на получената информация;

I.

4.4.1.2. Ежедневен мониторинг на UNIX/Linux базираните системи

- Наблюдение на наличността и работоспособността на операционната система;
- Наблюдение на състоянието на основните услуги на операционната система (daemons);
- Наблюдение на натоварването на процесорите;
- Наблюдение на количеството заета оперативна памет;
- Наблюдение на количеството заета swp памет;
- Наблюдение на зетото (свободно) дисково пространство;
- Наблюдение на натовареността на дисковата подсистема;
- Наблюдение на натоварването на мрежовите интерфейси;
- Анализ на получената информация;

4.4.1.3. Ежедневен мониторинг на виртуалната инфраструктура

- Наблюдение на наличността и работоспособността на виртуалните хостове;
- Наблюдение на натоварването на процесорите;
- Наблюдение на количеството заета (свободна) оперативна памет;
- Наблюдение на зетото (свободно) дисково пространство;
- Наблюдение на натовареността на дисковата подсистема;
- Наблюдение на натоварването на мрежовите интерфейси;
- Анализ на получената информация;

4.4.1.4. Ежедневно наблюдение на системните съобщения за грешки:

- Наблюдение за грешки и предупреждения в Event Logs на Windows базирани сървъри;
- Наблюдение за предупреждения и грешки в syslog, messages и daemon за Unix/Linux базирани сървъри;
- Наблюдение за предупреждения и грешки в логовете на устройствата от мрежовата инфраструктура;

4.4.1.5. Ежедневно наблюдение на състоянието на архивите:

- Наблюдение на състоянието на архивите на операционните системи чрез специализиран софтуер;
- Наблюдение на състоянието на архивите на 3rd party приложенията в ИТ инфраструктурата;
- Наблюдение на състоянието на архивите на СУБД;

4.4.1.6. Ежедневно наблюдение на състоянието на планираните задачи:

- Наблюдение на състоянието на Scheduled tasks;

- Наблюдение на състоянието на Crontab jobs;

4.4.1.7. Ежедневно наблюдение на състоянието на хардуера:

- Наблюдение на състоянието на хардуера, чрез специализиран централизиран софтуер, на всички устройства, които позволяват това;
- Наблюдение на състоянието на хардуера чрез специализиран софтуер предоставен от производителя на хардуера;

4.4.1.8. Администриране на Windows базирани системи:

- Администриране на MS Windows операционни системи;
- Инсталиране на нови закупени/наети MS Windows базирани сървъри;
- Конфигуриране на основни услуги предлагани от операционната система;
- Конфигуриране на хардуер на нови закупени/наети сървъри;
- Конфигуриране на планирани задачи (Scheduled tasks);
- Оказване на съдействие при инсталиране на 3rd party софтуер;
- Оказване на съдействие при конфигуриране на 3rd party софтуер;
- Възстановяване на работоспособността на ОС в случай на срив;

4.4.1.9. Администриране на Unix/Linux операционни системи:

- Администриране на Unix/Linux операционни системи;
- Инсталиране на нови закупени/наети Unix/Linux базирани сървъри;
- Конфигуриране на основни услуги предлагани от операционните системи;
- Конфигуриране на хардуер на нови закупени/наети сървъри;
- Конфигуриране на планирани задачи (Crontab jobs);
- Оказване на съдействие при инсталиране на 3rd party софтуер;
- Оказване на съдействие при конфигуриране на 3rd party софтуер;
- Възстановяване на работоспособността на ОС в случай на срив;

4.4.1.10. Администриране на виртуална инфраструктура

- Инсталиране, конфигуриране и поддръжка на нови и съществуващи виртуални хостове (Virtual Hosts);
- Конфигуриране и администриране на виртуални мрежи (VLANs);
- Конфигуриране и администриране на достъп до локални и споделени дискови масиви;
- Администриране и конфигуриране на достъпа до виртуалната инфраструктура;
- Администриране на правата на администраторите/потребителите и нивата на достъп, с които разполагат;
- Администриране и конфигуриране на виртуални машини. Създаване, изтриване на виртуални машини. Конфигуриране на необходимите ресурси за нуждите на виртуалната машина;
- Конфигуриране на права за достъп до виртуалните машини;
- Конфигуриране на Templates за автоматизирано създаване на виртуални машини по предварително зададени параметри;

- Конфигуриране и администриране на автоматично създаване на Snapshots на виртуални машини;

4.4.1.11. Администриране на сървърите обслужващи СУБД:

- Администриране и поддръжка на системите за управление на бази от данни;
- Ежедневен контрол на еталонните параметри и работоспособността на СУБД;
- Възстановяване на работоспособността на СУБД в случай на срив;
- Възстановяване на данни в случай на загуба или повреждане;
- Администриране и поддръжка на сървърни приложения, в частта им взаимодействаща с базите данни;

4.4.1.12. Администриране на архивите

- Архивиране на данни по предварително изготвена архивна схема спрямо нуждите на сървърните приложения;
- Създаване на нови архивни задачи чрез специализиран софтуер;
- Конфигуриране и промяна в конфигурацията при необходимост на архивните задачи;
- Конфигуриране и промяна в конфигурацията при необходимост на архивните задачи за архивиране на СУБД;
- Отстраняване на възникнали проблеми с архивите;
- Оказване на съдействие при конфигурирането на архивите на 3rd party софтуер чрез специализирани за него инструменти;
- Поддръжка на специализиран софтуер за архивиране;
- Възстановяване на информация от архив при необходимост;
- Управление на смяната на архивни ленти и други носители;
- Тестово възстановяване от архив в случай на срив на системите;

4.4.1.13. Поддръжка на хардуера

- Диагностика на проблеми със сървърния хардуер с помощта на специализирани инструменти предоставени от производителя на хардуера;
- Инсталиране и конфигуриране на нови хардуерни компоненти (цената на компонентите не е включена в цената на услугата);
- Инсталиране и конфигуриране на нови сървъри и устройства(цената на сървърния хардуер и устройства не е включена в цената на услугата);

4.4.1.14. Администриране на кръпки по сигурността (Security Patches Management):

- Тестване на кръпки по сигурността за различните видове приложения и операционни системи;
- Инсталиране на одобрените кръпки за различните видове приложения и операционни системи;
- Оказване на съдействие при необходимост от инсталация на кръпки/обновяване на версии на 3rd party приложения;

4.4.2. По отношение на инфраструктурните услуги ИЗПЪЛНИТЕЛЯТ е длъжен да осигури следното:

4.4.2.1. Мониторинг и поддръжка на Microsoft Active Directory:

- Мониторинг на Active Directory услугата;
- Мониторинг на репликацията между домейн контролерите;
- Ежемесечни проверки и профилактика на тестовата и продукционната среда;
- Инсталиране и конфигуриране на нови Domain Controllers (DC);
- Премахване (Demote) на Domain Controllers (DC);
- Администриране на активната директория по установени еталони и модели;
- Създаване, конфигуриране и управление на Group Policy Objects (GPOs);
- Създаване, конфигуриране и поддръжка на структурата на Organizational Units (OUs);
- Създаване, конфигуриране и поддръжка на Security Groups (SG);
- Създаване и администриране на потребителски акаунти (User accounts);
- Следене на актуалността на дефинираните потребители и предоставяне на информация за това на ВЪЗЛОЖИТЕЛЯ;
- Поддръжка на справки за потребителите в Active Directory;
- Управление на AD Site Topology;
- Управление на Active Directory Domains;
- Управление на Operation Masters;
- Управление на схемата на Active Directory;
- Отстраняване на външни проблеми, като в случай на необходимост действията ще бъдат съгласувани с външни организации;
- Архивиране и възстановяване на данните в Active Directory;

4.4.2.2. Мониторинг и поддръжка на DNS услугата:

- Мониторинг на състоянието на DNS услугата;
- Мониторинг на състоянието на DNS сървърите;
- Инсталиране, конфигуриране и поддръжка на DNS сървъри;
- Премахване на инсталирани DNS сървъри;
- Създаване, конфигуриране и поддръжка на прави и обратни вътрешни и външни DNS зони;
- Архивиране и възстановяване на DNS услугата;

4.4.2.3. Мониторинг и поддръжка на WINS услугата:

- Мониторинг на състоянието на WINS услугата;
- Мониторинг на състоянието на WINS сървърите;
- Инсталиране, конфигуриране и поддръжка на WINS сървъри;
- Премахване на инсталирани WINS сървъри;

4.4.2.4. Мониторинг и поддръжка на DHCP услугата:

- Мониторинг на състоянието на DHCP услугата;
- Мониторинг на състоянието на DHCP сървърите;
- Инсталиране, конфигуриране и поддръжка на DHCP сървъри;

- Създаване, конфигуриране и поддръжка на DHCP Scopes;
 - Архивиране и възстановяване на DHCP услугата;
- 4.4.2.5. Мониторинг и поддръжка на файлови сървъри:
- Мониторинг на достъпа до файловите сървъри. Следене за неоторизиран достъп до информацията на файловите сървъри;
 - Инсталиране, конфигуриране и поддръжка на файлови сървъри под различни операционни системи;
 - Интеграция на услугата File Sharing с Microsoft Active Directory;
 - Споделяна на папки;
 - Конфигуриране и управление на права за достъп до споделените папки;
 - Конфигуриране и управление на квоти за отделните потребители на ниво дял и папка;
 - Поддръжка на актуален архив на информацията в споделените папки;
- 4.4.2.6. Мониторинг и поддръжка на PKI
- Мониторинг на състоянието на PKI услугата;
 - Мониторинг на състоянието на PKI сървъра;
 - Инсталиране, конфигуриране и поддръжка на PKI сървъри;
 - Управление на сертификати (издаване, анулиране);
 - Управление на Certificate Templates;
 - Архивиране и възстановяване на PKI услугата;
 - Мониторинг и администриране на Microsoft SharePoint Server
 - Мониторинг на състоянието на SharePoint услугата. Наблюдение на еталонните и параметрите;
 - Мониторинг на състоянието на SharePoint сървъра;
 - Инсталиране, конфигуриране и поддръжка на SharePoint сървъри (не включва администрирането и разработването на SharePoint Sites и приложения);
 - Архивиране и възстановяване на SharePoint услугата;
- 4.4.2.7. Мониторинг и администриране на WEB сървъри:
- Мониторинг на състоянието на WEB услугите;
 - Мониторинг на състоянието на сървърите, предлагащи WEB услуги;
 - Инсталиране, конфигуриране и поддръжка на WEB сървъри (не включва администриране и разработването на WEB приложения);
 - Архивиране и възстановяване на WEB услуги;
- 4.4.2.8. Мониторинг и администриране на пощенска услуга:
- Мониторинг на състоянието на пощенската услуга;
 - Мониторинг на състоянието на пощенските сървъри;
 - Мониторинг на състоянието на базите;
 - Мониторинг на състоянието на базите с опашки от писма;
 - Инсталиране, конфигуриране и поддръжка на пощенски сървъри и сървъри, които са необходими за нормалното функциониране на пощенската услуга;
 - Управление на конфигурацията на пощенската услуга;

- Поддръжка на базите с пощенските кутии на потребителите;
- Поддръжка на базите с опашки от писма;
- Конфигуриране и управление на Anti-Spam защитата на пощенската услуга;
- Провеждане на тестове в тестова среда преди промяна в конфигурацията на пощенската услуга;
- Архивиране и възстановяване на конфигурацията на пощенската услуга;
- Ежедневно архивиране на базите с потребителски пощенски кутии;

4.4.3. По отношения на специализирания приложен софтуер ИЗПЪЛНИТЕЛЯТ следва да осигурява следните дейности:

- 4.4.3.1. Инсталиране на специализиран приложен софтуер на сървърите при закупуване или подмяна на технически и програмни средства;
- 4.4.3.2. Обновяване на инсталирания приложен софтуер;
- 4.4.3.3. Периодично наблюдение и осигуряване на нормалното функциониране на специализираните приложни системи;
- 4.4.3.4. Администриране на приложен софтуер – поддържане на актуални потребители и други административни функции;
- 4.4.3.5. Оказване на системна помощ на потребителите на специализираните приложни системи;

Цялата необходима документация, както и дистрибутивите на софтуера за инсталиране и преинсталиране на наличните специализирани приложни системи и дефиниране на информационни структури и номенклатури в тях се предоставят от МОН.

4.4.4. По отношение на базите от данни ИЗПЪЛНИТЕЛЯТ следва да осигури следните дейности:

- 4.4.4.1. Наблюдение на често повтарящи се грешки, които биха могли да доведат до нарушение на работоспособността на базата от данни и тяхното своевременно отстраняване. Проучване на възможните грешки и последствия за базата данни при обновяване на версията и възможностите за оптимизация при преминаване към по-нова версия. Периодичен контрол на еталонните параметри и работоспособността на базата от данни.
- 4.4.4.2. Администриране на наличните бази от данни по установени еталони и модели;
- 4.4.4.3. Промяна на системни настройки - след съгласуване с МОН;
- 4.4.4.4. Отстраняване на възникнали проблеми, като в случай на необходимост действията се съгласуват с външни организации;
- 4.4.4.5. Ежемесечни проверки и профилактика на тестовата и продукционната среди;
- 4.4.4.6. Ежедневно архивиране на статистическите файлове;
- 4.4.4.7. Архивиране и възстановяване на базите;

- 4.4.5. По отношение на сигурността на информацията ИЗПЪЛНИТЕЛЯТ следва да осигури следните дейности:
- 4.4.5.1. Прилагане на политиката и процедурите за сигурност на информационните системи на МОН;
- 4.4.5.2. Непрекъснат контрол и известяване на МОН по отношение на:
- Осъществяване на пробив или опит за пробив в системата, хакерски атаки или проникване на вируси;
 - Неоторизирано протичане или копиране на информация, опит за кражба на потребителски имена, пароли, лични данни и друга поверителна информация;
 - Неоторизирано записване на данни и информация или унищожаване на такава;
- 4.4.6. ИЗПЪЛНИТЕЛЯТ трябва да осъществява контакт с всички доставчици на ИТ решения, които работят в мрежата на МОН
- 4.4.7. ИЗПЪЛНИТЕЛЯТ е длъжен да асистира на доставчиците на 3rd party приложения и решения при интегрирането им в ИТ инфраструктурата на МОН
- 4.4.8. ИЗПЪЛНИТЕЛЯТ е длъжен да изготвя аргументирани предложения за подобрене на ИТ инфраструктурата на МОН
5. Администриране, поддържане и развитие на комуникационното оборудване в мрежата на МОН
- 5.1. Дейности по предоставянето на услугата
- 5.1.1. ИЗПЪЛНИТЕЛЯТ следва да осигури поддръжка на комуникационното оборудване със следните функции:
- 5.1.1.1. Осъществяване на 24 часово наблюдение на работоспособността на комуникационното оборудване. Регистриране и локализация на повреди в активното оборудване. Координиране на действията при отстраняване на повреди, включително с външни доставчици на оборудване и съединителни връзки;
- 5.1.1.2. Конфигурация и преконфигурация на комуникационното оборудване и преносната среда. Сваляне и запазване на конфигурациите на активното мрежово оборудване. Поддържане на база от данни за текущите и миналите конфигурации на активното оборудване.
- 5.1.1.3. Провеждане на тестове в тестова среда при необходимост от значима промяна в конфигурацията;
- 5.1.1.4. Наблюдение и анализ на функционирането на комуникационното оборудване. Измерване и анализ на параметрите на трафика и предложения за оптимизации на комуникационното оборудване;
- 5.1.1.5. Поддържане на актуална база данни относно видовете активно оборудване, комуникационни връзки и др.;

- 5.1.1.6. Създаване и поддръжка на система за мониторинг на работоспособността на комуникационното оборудване и връзките на МОН и своевременно уведомяване при възникнали проблеми.
- 5.1.2. ИЗПЪЛНИТЕЛЯТ е длъжен да поддържа и администрира следните специализирани връзки
 - 5.1.2.1. Всички връзки с НАМДА;
 - 5.1.2.2. Всички връзки с външни доставчици на интернет свързаност;
- 6. Администриране, поддръжка и развитие на АИС за работа с класифицирана информация
 - 6.1. Дейности по предоставянето на услугата
 - 6.1.1. По отношение на АИС за работа с класифицирана информация ИЗПЪЛНИТЕЛЯТ следва осигури:
 - 6.1.1.1. Инсталиране, конфигуриране и поддръжка на АИС за работа с класифицирана информация по установени процедури;
 - 6.1.1.2. Администриране на АИС за работа с класифицирана информация
 - 6.1.1.3. Администриране на права за достъп до АИС за работа с класифицирана информация;
 - 6.1.1.4. Осигуряване на непрекъсната работа на АИС за работа с класифицирана информация;
 - 6.1.1.5. Архивиране на АИС за работа с класифицирана информация по установени процедури.
 - 6.2. Всички дейности по т. 6.1. следва да се извършват от експерти на изпълнителя, притежаващи разрешение за достъп до класифицирана информация ниво „Поверително“, съгласно ЗККИ;
 - 7. Технически средства за осъществяване на услугите
 - 7.1. Средства за управление на системната поддръжка
 - 7.1.1. Да работи 24 часа в денонощието, 365 дни в годината;
 - 7.1.2. Да има минимум 6 канала за достъп - електронна уеб-базирана система за регистриране и обработване на инциденти, уеб-портал за споделяне на документи, мобилен телефон, стационарен телефон, факс, e-mail;
 - 7.1.3. Да има съществуващи нива за ескалация на постъпилите заявки;
 - 7.2. Имплементиране на мониторинг система

Изпълнителят следва да предложи и въведе използването на мониторинг система за следене на състоянието на услугите и оборудването със следните минимални изисквания:

7.2.1. Да може да се извършва мониторинг на следните сървърни хардуерни компоненти:

- Наблюдение на дискови контролери;
- Наблюдение на състоянието на батериите на кеша на дисковите контролери;
- Наблюдение на състоянието на кеша на дисковите контролери;
- Наблюдение на физическите дискове;
- Наблюдение на конфигурираните логически дискове;
- Наблюдение на състоянието на процесорите;
- Наблюдение на състоянието на системните вентилатори;
- Наблюдение на състоянието на захранващите блокове на системата;

7.2.2. Да може да извършва мониторинг на следните операционни системи и компоненти:

- Microsoft Windows операционни системи – Windows Server 200, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012;
- Linux / Unix операционни системи – FreeBSD, Ubuntu Linux, Debian Linux, Red Hat Linux;
- Наблюдение на основните параметри на операционните системи следвайки добрите практики за съответната операционна система – натоварване на процесорите на системата, натоварване на дисковата подсистема, наблюдаване на свободното / заето дисково пространство, наблюдаване на свободната / заета оперативна памет, наблюдение на основните параметри на виртуалната памет на операционните системи и други;
- Наблюдение на състоянието на сервизите / демоните на операционните системи;
- Наблюдение на основните параметри на инфраструктурните услуги следвайки добрите практики за съответната операционна система – DNS, DHCP, PKI, Active Directory и др.;
- Наблюдение на основните параметри на сървърни приложения – Microsoft Exchange Server, Microsoft SQL Server, IIS, SharePoint, Apache и др.;
- Наблюдение на системните логове на сървърните операционни системи – Application Log, System Log, Security Log, Sys Log, специализирани логове на инсталирания софтуер и др.;

7.2.3. Да може да извършва наблюдение на мрежовото оборудване – наблюдение на наличността на мрежовите устройства, наблюдение на натоварването на процесора, наблюдение на количеството заета / свободна оперативна памет, наблюдение на трафика през интерфейсите на устройствата;

- 7.2.4. Да може да извършва наблюдение на комуникационната свързаност, както към външни доставчици, така и към отдалечени звена в мрежата на МОН и да известява автоматично при отпадане на свързаността;
- 7.2.5. Мониторинг системата да следи параметрите на оборудването 24 часа в денонощието, 7 дни в седмицата;
- 7.2.6. Информацията от мониторинга да се запазва в база данни, която да позволява извършване на справки за изминали периоди от време;
- 7.2.7. Да може да бъде изпращана автоматична нотификация по e-mail при достигане на гранични стойности на наблюдаваните параметри;
- 7.2.8. Мониторинг системата да позволява конфигурирането на потребителски акаунти с различни нива на достъп;
- 7.2.9. Мониторинг системата да позволява графично визуализиране на събраните данни за наблюдаваните параметри с динамично определяне на интервала от време, за който да се визуализират данните;
- 7.2.10. Мониторинг системата да позволява визуализирането на физическото местонахождение на устройствата и връзките между тях чрез карта на мрежата (network map);

РАЗДЕЛ II. ПРИЛОЖЕНИЕ КЪМ ТЕХНИЧЕСКОТО ЗАДАНИЕ

ПРИЛОЖЕНИЕ 1А – Гарантирани параметри на услугата и технически изисквания

1. Гарантирани параметри на услугата и технически изисквания по точки 4, 5 и 6.

	Параметър	Тип изискване	Описание / Изискване
1.1	Изискване към предоставяне на услугата		
	Обслужване и достъпност на каналите за заявяване на поддръжка (24 часа в денонощието, 7 дни в седмицата, 365 дни в годината)	Точно	Задължително
	Време за реакция при критичен инцидент, застрашаващ работата на цялата система	Максимум	1 час
	Време за реакция при инцидент, застрашаващ отделни резервирани компоненти на системата	Максимум	4 часа
	Време за реакция при инцидент, застрашаващ отделни нерезервирани компоненти на системата, с некритичен статус	Максимум	8 часа
	Време за отстраняване на критичен инцидент, застрашаващ работата на цялата системата	Максимум	8 часа
	Време за отстраняване на инцидент, застрашаващ отделни резервирани компоненти на системата	Максимум	24 часа
	Време за отстраняване на инцидент, застрашаващ отделни нерезервирани компоненти на системата, с некритичен статус	Максимум	5 работни дни
	Осигуряване на минимум двама души, които ежедневно в рамките на работното време на ВЪЗЛОЖИТЕЛЯ от 09:00 до 17:30 да се ангажират на място с поддръжка.	Точно	Задължително
2.1	Изисквания към предоставяне на услугата		
	Възможност за приемане на заявки за поддръжка по телефон или други гласови канали и ръчно отваряне на „инциденти” през операторски интерфейс	Точно	Задължително

	Възможност за приемане на заявки по безплатен телефон за обслужване на потребителите от тип 0800 XXX	Точно	Задължително
	Възможност за приемане на заявки за поддръжка по e-mail.	Точно	Задължително
	Възможност за приемане на заявки за поддръжка през уеб-базирана система за регистриране и обработване на инциденти, която използва SSL (доказва се с линк или работен екран от системата, която удостоверява използването на SSL сертификата)	Точно	Задължително
	Възможност за автоматична нотификация по e-mail при развитие на всеки „инцидент“	Точно	Задължително
	Отчетност и статистика за постигнатите параметри на поддръжка (времена за реакция, времена за затваряне на „инцидента“ и пр.)	Точно	Задължително
	Наличие на уеб-портал за споделяне на файлове, документи, контакти, графици и календари за изпълнение на услуги, планирани задачи за поддръжка (доказва се с работни екрани от системата, удостоверяващи въвеждането на файлове, документи, контакти, планирани мероприятия в календар, новини по проекта или важни предстоящи събития)	Точно	Задължително
	Възможност за създаване на общ график за планиране на повтарящи се (регулярни) дейности по профилактика и поддръжка. Възможност за автоматични нотификации при приближаване на зададените в графика дати	Точно	Задължително
	Наличие на тестова среда с минимум 52 процесорни ядра и 96 GB RAM (доказва се с работни екрани на физическата платформа от Virtual Center или Microsoft VMM)	Точно	Задължително



ПРИЛОЖЕНИЕ 2А – Описание на техническата и програмна среда в системата на МОН

2. Оборудване и софтуер в обхвата на услугата по точки 4, 5 и 6

Оборудване	Брой
Virtual servers	11
Supermicro X7DBU	2
Supermicro X7DB8	1
ProLiant MicroServer	1
Intel Sapello S5000VSA	2
Intel Rolling Prairie SE7525RP2	1
IBM System x3650 M3	1
IBM System x3650 M2	2
HP ProLiant ML350 G4	1
HP ProLiant DL360 G5	1
HP ProLiant DL180 G6	1
Dell PowerEdge 2950	6
Dell PowerEdge 2600	1
Dell PowerEdge 1800	1
Други	3

Операционни системи	Брой
Microsoft Windows	30
Linux	5

Приложения	Брой
Виртуална среда VMWare ESXi	1
Виртуална среда Microsoft Hyper-V	5
Софтуер за архивиране Microsoft DPM 2007/2010	4
Microsoft Exchange 2007 Server	2
Web Server	13
Microsoft SharePoint Server	1
Symantec Antivirus Server	1
Microsoft WSUS Server	1
Microsoft CA	1
Database Server	15

Комуникационно оборудване/Модел	Брой
Cisco Catalyst 2950-48 G	7
Cisco Catalyst 2950-24 G	4
Cisco Catalyst C3750X -24 G	1
Cisco Catalyst C3560C -8PC-S	3
Cisco Catalyst C3560 -8PC-S	1
Cisco Catalyst 3550-12 G	1
Cisco Catalyst 2960G-24	1
Cisco Catalyst 2960-24TC-L	1
Cisco Catalyst 2960-48TC-S	2
Cisco Catalyst 2950-24	2

Catalyst 2960 24 10/100, 2T/SFP	1
Catalyst 2960 24 10/100/1000, 4 T/SFP	1
ASA 5540 with AIM SSM 20	1
CISCO2921/K9	1
Cisco 1200 Access Point	6

II. Критерий за оценка – най – ниска предложена цена.

III. Прогнозна стойност за извършване на услугата – до 66 000 (шестдесет и шест хиляди) лева без ДДС.

IV. Срок за изпълнение – 12 месеца

V. Изисквания към участниците:

1. Всеки участник трябва да разполага с център за техническа поддръжка работещ 24 часа в денонощието, 7 дни в седмицата, 365 дни в годината и работеща „trouble ticket“ („съобщение за проблеми“) система с ясна схема за реакция и своевременно отстраняване на възникнали проблеми. Центърът трябва да поддържа минимум 6 канала за достъп - електронна уеб-базирана система за регистриране и обработване на инциденти, уеб-портал за споделяне на документи, мобилен телефон, стационарен телефон, факс, e-mail. Участникът трябва да представи описание на предлаганата от него поддръжка.
2. Всеки участник трябва да има минимум 2 (два) сключени договора за поддръжка с гарантирани параметри на обслужване (SLA) на Системна платформа или Информационна система, които обслужват минимум 200 потребители (общо за всички договори) на обща стойност минимум 50 000 (петдесет хиляди) лева без ДДС.
3. Всеки участник трябва да работи по сертифицирана система за управление на качеството по стандарта ISO 9001:2008 или еквивалентен.
4. Всеки участник трябва да работи по сертифицирана система за управление на информационната сигурност по стандарта ISO 27001:2005 или еквивалентен.
5. Всеки участник трябва да притежава ISO/IEC 20000:2005 за информационни технологии и управление на услугите или еквивалентен.
6. Всеки участник трябва да разполага с офис на територията на гр. София – участникът следва да представи декларация за доказване на това обстоятелство с точен адрес на офиса.
7. Екипът от специалисти на всеки участник трябва да бъде съставен от минимум 6 (шест) висококвалифицирани специалисти, със следната квалификация:
 - a. Ръководител проект със следните умения и квалификация:

- i. Диплома за висше образование магистърска степен;
 - ii. Минимум 5-годишен опит в управлението на проекти в сферата на информационните технологии;
 - iii. Притежава сертификат за управление на проекти, съгласно световно утвърдена методология за управление на проекти (Project Management Professional, PRINCE2 Practitioner или IPMA Level B/A);
 - iv. да е член на утвърдена международна организация от професионалисти в областта на управление на проекти;
 - v. Участие като ръководител проект в минимум 5 успешно приключени проекта за разработване и внедряване на интегрирани информационни системи;
- b. Експерт, поддръжка сървърна инфраструктура и администриране и поддръжка на АИС за работа с класифицирана информация със следните умения и квалификация:
- i. VMWare Certified Professional;
 - ii. MCITP: Enterprise Administrator on Windows Server 2008 или по-висок;
 - iii. разрешение за достъп до класифицирана информация ниво „Поверително“, съгласно ЗККИ;
- c. Експерт поддръжка на сървърна инфраструктура със следните умения и квалификация:
- i. MCTS: Microsoft Exchange Server 2010 или по-висок;
 - ii. MCSA: Windows Server 2012 или MCITP: Enterprise Administrator on Windows Server® 2008 или по-висок;
 - iii. MCITP: Virtualization Administrator on Windows Server 2008 R2 или по-висок;
- d. Експерт, поддръжка на бази данни със следните умения и квалификация:
- i. MCITP: Enterprise Administrator on Windows Server® 2008 или по-висок;
 - ii. MCTS: SQL Server 2005 или по-висок;
- e. Експерт, поддръжка на мрежа със следните умения и квалификация:
- i. CCIE;
- f. Експерт, поддръжка на мрежа със следните умения и квалификация:
- i. CCNP;

Доказва се с приложени договор/автобиографии/сертификати.

8. Всеки участник трябва да удостовери наличието на лаборатория /тестов център/ където биха могли да се изпробват промени в ИС на Възложителя, преди да бъдат извършени в продукционната му среда.
9. Всеки участник следва да осигури минимум двама души, които ежедневно в рамките на работното време на Възложителя от 9.00 ч. до 17.30 ч. да се ангажират на място с поддръжката на и отстраняване на проблеми с информационната инфраструктура на МОН (сървъри, мрежа и специализирано

оборудване), проверка параметрите на микроклимата в сървърни помещения, администриране на операционните системи и на системите за управление на базите от данни, администриране на приложен софтуер, администриране на дисковото пространство с цел оптималното му използване и регистриране на повреди в активното оборудване.

10. Участникът трябва да представи конкретен и подробен план и описание на дейностите необходими за извършване на поддръжката, както и документ, описващ процеса, който ще бъде използван при извършване на поддръжката;
11. Участника трябва да представи план за управление на риска в хода на проекта, в които да е оценил възможните рискове и подробно е описал възможните влияния като особено внимание е обърнато на плавното продължаване на работата при решаване на инцидент. В плана трябва да има подробно описание на мерките за смекчаване на последствията от рисковете.