Приложение № 1

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

за

„Привеждане на информационните активи на НСИ в съответствие с изискванията на Евростат и миграция към ХЧО“ включваща доставка, монтаж, пускане в експлоатация и гаранционно обслужване“

1. Текущо състояние

В Националния статистически институт (НСИ) се използват предимно стари физически сървърни системи, дискови масиви, устройства за осигуряване на комуникацията, устройства и системи за създаване на архиви. Техниката е от различни производители и с изтекло гаранционно обслужване и сервиз. Част от използваните устройства са изтеглени от пазарните листи на производителите. Сървърната инфраструктура е разположена в ЦУ на НСИ. Състои се от виртуални платформи и самостоятелни сървъри.

1.1. Виртуална среда под управлението на VMware със следните ресурси:

- брой ядра –136 процесорни ядра;
- общо оперативна памет – 1120 GB;
- общ брой хостове – 8;
- използвано дисково пространство – 30 TB в две дискови подсистеми с iSCSI и FC свързаност;
- общ брой виртуални машини – 78.

1.2. Виртуална среда под управлението на Hyper-V със следните ресурси:

- брой ядра – 12 процесорни ядра;
- общо оперативна памет – 64 GB;
- общ брой хостове – 2;
- използвано дисково пространство – 10 TB с iSCSI свързаност;
- общ брой виртуални машини – 7.

1.3. Хардуерни сървъри със следните ресурси:

- брой ядра 31 процесорни ядра;
- общо оперативна памет – 192 GB;
- общо дисково пространство – 15 TB, като се използват локални дискове и дискови подсистеми с FC свързаност;
- общ брой хостове – 18.

1.4. Комуникационната инфраструктура в ЦУ е разделена на отделни сегменти:

- периметър зона (Perimeter zone) – това е зоната, чрез която се осъществява връзка към външни за НСИ комуникационни инфраструктури. В нея са включени следните устройства – резервирана двойка периметър комутатори Cisco 2960X, резервирана двойка маршрутизатори Cisco ASR 1001X, както и резервирана двойка защитни стени Cisco ASA 5525X;
- зони за сигурност (DMZ) – обособени са зони за сигурност. Трафикът между тях и останалите сегменти от мрежата се контролира с помощта на двойката защитни стени Cisco ASA 5525X;
- гръбнак на мрежата (Core segment) – гръбнакът на мрежата е изграден с помощта на двойка опорни комутатори Cisco 3850. Те осигуряват надеждна и висикоскоростна Layer 3 връзка между всички мрежови сегменти;
- сегмент за обработка на данни (Datacenter segment), в който се използват двойка дейтацентър комутатори Cisco Nexus 5672UP с разширители Cisco Nexus 2232 и двойка SAN комутатори Cisco MDS 9148. Комутаторите в този сегмент не са оборудвани с интерфейсни разширителни модули (SFP);
- сегмент за достъп (Access segment) – в този сегмент са разположени потребителските работни станции принтери и т.н. Той е изграден с помощта на комутатори Cisco 2960X и Cisco SG300, които са свързани към опорните комутатори Cisco 3850.

2. Очаквани резултати

Изградената нова инфраструктура на НСИ ще увеличи капацитета и възможностите на държавния хибриден частен облак, чрез осигуряване на сървърна инфраструктура, инфраструктура за съхранение на данни, софтуер за създаване и управление на резервни копия и мрежови компоненти, осигуряващи допълнителна свързаност, подобряване на информационна и кибер-сигурност, гарантиране на конфиденциалност и интегритет на информационните активи на НСИ, защитата на личните данни и управлението на инфраструктурата.

Новата инфраструктура ще е изградена от четири градивни блока:

- сървърна инфраструктура – основа за сървърна виртуализация, която ще консолидира всички приложения, сървъри и бази данни на НСИ;
- инфраструктура за съхранение на данни – базирана на дискови масиви използващи дискове с различни капацитети и скорост в зависимост от функционалната си роля;
- софтуер за създаване и управление на резервни копия;
- мрежови компоненти осигуряващи допълнителна свързаност и мрежова сигурност.

2.1. Сървърна инфраструктура

Сървърната инфраструктура ще е базирана на стандартни x86 сървъри. Сървърите ще образуват два отделни виртуализирани клъстера както следва:

- два от сървърите ще бъдат предназначени за Oracle базираните приложения и бази данни. Върху тях ще бъде инсталирана и конфигурирана Oracle VM виртуализация, което ще позволи оптимизация на специфичното Oracle лицензиране;
- останалите сървъри ще образуват общ виртуален клъстер, базиран на предложен от участника софтуер за сървърна виртуализация. Клъстерът ще предостави общ ресурс за всички останали приложения, сървъри и бази данни на НСИ.

Всички сървъри ще бъдат осигурени със съответните мрежови модули за връзка към съществуващата 10 Gbps сървърна Ethernet мрежа и 16 Gbps FC модули за връзка към съществуващата SAN инфраструктура.

2.2. Инфраструктура за съхранение на данни

Инфраструктурата за съхранение на данни ще бъде базирана дискови масиви, които ще бъдат разделени функционално, спрямо вида на използваните дискове и добрите практики:

- дисков масив тип 1 ще е изцяло Flash базиран. Капацитета ще се използва за приложения и бази данни, които изискват голяма производителност на дисковите операции. На него ще са разположени операционните системи на виртуални машини;
- дисков масив тип 2 ще предостави стандартно автоматично разпределение на капацитет върху бързи SAS и бавни NL SAS дискове. Този капацитет ще се използва за приложения и процеси, за които не е критична производителността на дисковите операции;
- дисков масив тип 3 ще се използва от системата за съхранени и управление на резервни копия и ще бъде съставен от бавни NL SAS дискове с висок капацитет. Този дисков масив ще покрие добрата практика, резервните копия да се съхраняват отделно от работните данни.

Дисковите масиви ще бъдат свързани към съществуващата SAN инфраструктурата.

2.3. Софтуер за създаване и управление на резервни копия

За защита на операционните системи, сървърите и приложенията, работещи на новата инфраструктура, ще се изгради система за защита на данните чрез създаване и управление на резервни копия. Софтуерът ще поддържа виртуална инфраструктура, и ще създава резервни копия на виртуалните машини. Допълнително, системата ще се интегрира с Oracle, Microsoft SQL, Informix, MySQL бази данни, за по-добрата им защита. Всички резервни копия ще се съхраняват на предвидения за това Дисков масив тип 3. За нуждите на архивирането на информацията, софтуерът ще поддържа и съхранение на копията на ленти или лентови библиотеки.

2.4. Мрежови компоненти

За управление и свързаност на новите компоненти, ще се използва мрежово устройство, което ще консолидира в себе си всички точки за управление. За защита на цялата мрежова инфраструктура ще се добави и специализирана система за мрежова сигурност за идентифициране на потребителите и крайните устройства в мрежата, и управление на достъпа.

3. Минимални технически изисквания

№	Описание / параметър / компонент	Изискване
1.	**Сървър тип 1 – 2 броя**	
1.1.	Общо описание, производител, модел	Да се предостави физически сървър предназначен за сървърна виртуализация (Oracle VM)
1.2.	Форм фактор, задължително	За монтаж в стандартен 19“ шкаф, минимум 2RU
1.3.	Процесор, задължително	Инсталирани 2 броя процесори, 14 ядра, 2.4 GHz, последно поколение Xeon E5 v4 или еквивалентен
1.4.	Оперативна памет, минимум	512 GB, 2400MHz
1.5.	Оперативна памет, поддръжка	Минимум 1.5 TB

№	Описание / параметър / компонент	Изискване
1.6.	Капацитет за операционна система, минимум	2 броя HDD, 300 GB 10K 12 Gbps SAS, конфигурирани в RAID 1 група
1.7.	Свързаност, LAN, минимум	2 порта 10GBase-T 4 порта 1 Gbps
1.8.	Свързаност, SAN, минимум	2 порта FC 16 Gbps
1.9.	Разширителни модули, минимум	8 броя PCIe 3.0
1.10.	Захранване, задължително	Резервирано, AC 220-240V
1.11.	Управление, задължително	С включен лиценз за отдалечено управление чрез WEB, с възможност за KVM конзола и емулация на CD/DVD
1.12.	Допълнителни кабели и модули, задължително	Да се достави със всички кабели за свързването му към инфраструктурата
1.13.	Гаранция – минимум, реакция – максимум	3 години от производителя, с поддръжка в работно време и време за реакция до 4 часа.
2.	**Сървър тип 2 – 8 броя**	
2.1.	Общо описание, производител, модел	Да се предостави физически сървър предназначен за сървърна виртуализация
2.2.	Форм фактор, задължително	За монтаж в стандартен 19“ шкаф, минимум 2RU
2.3.	Процесор, задължително	Инсталирани 2 броя процесори, 14 ядра, 2.4 GHz, последно поколение Xeon E5 v4 или еквивалентен
2.4.	Оперативна памет, минимум	512 GB, 2400MHz
2.5.	Оперативна памет, поддръжка	Минимум 1.5 TB
2.6.	Капацитет за операционна система	Да се предостави капацитет за инсталиране на операционна система за виртуализация (диск, USB flash, SD)
2.7.	Свързаност, LAN, минимум	2 порта 10GBase-T 4 порта 1 Gbps
2.8.	Свързаност, SAN, минимум	2 порта FC 16 Gbps
2.9.	Разширителни модули, минимум	8 броя PCIe 3.0
2.10.	Захранване, задължително	Резервирано, AC 220-240V
2.11.	Управление, задължително	С включен лиценз за отдалечено управление чрез WEB, с възможност за KVM конзола и емулация на CD/DVD
2.12.	Допълнителни кабели и модули, задължително	Да се достави със всички кабели за свързването му към инфраструктурата
2.13.	Гаранция – минимум, реакция – максимум	3 години от производителя, с поддръжка в работно време и време за реакция до 4 часа.
3.	**Дисков масив тип 1 – 1 брой**	
3.1.	Общо описание, производител, модел	Да се предложи дисков масив с изцяло Flash базирана Scale-Out архитектура. Решението трябва да използва Scale-Out технология, при която при добавянето на капацитет линейно се разширяват и останалите компоненти на системата (памет, процесорна мощ, портове и др.)

№	Описание / параметър / компонент	Изискване
3.2.	Форм фактор	За монтаж в 19“ шкаф
3.3.	Контролери за управление	Резервирани контролери за управление
3.4.	Общ капацитет	10 TB Raw капацитет съставен изцяло от SSD (FLASH) дискове
3.5.	Използваем капацитет	7.5 TiB
3.6.	Защита на данните	Възможност за едновременно отпадане на 2 диск без загуба на данни
3.7.	Свързаност	Мин. 4 x 8 Gbps FC Мин. 4 x 10 Gbps Ethernet ISCSI Мин. 2 x 1 Gbps за управление
3.8.	Функционалност включена в предложението	Да поддържа Data Deduplication (inline) Да поддържа Data Compression (inline) Да поддържа Thin Provisioning Да поддържа Snapshots в това число: Консистентни групи – възможност за създаване на едновременен Snapshot на група от дялове Snapshots предназначени само за четене Snapshots с възможност за използването им за четене и писани (като стандартни дялове)
3.9.	Функционалност (Възможност)	Възможност за криптиране на данните чрез SED – самокриптиращи се дискове
3.10.	Захранване	Резервирано захранване, AC 220 – 240 V
3.11.	Обновяване на системата	Обновяването на системния софтуер да е без нужда от прекъсване на работата на масива
3.12.	Управление	Да предоставя управление посредством GUI (графичен интерфейс) Да предоставя управление посредством CLI (команден ред)
3.13.	Допълнителни кабели и модули, задължително	Да се достави със всички кабели за свързването му към инфраструктурата
3.14.	Гаранция – минимум, реакция – максимум	3 години от производителя, с поддръжка 24x7 и време за реакция до 4 часа.
4.	**Дисков масив тип 2 – 1 брой**	
4.1.	Общо описание, производител, модел	Да се предостави дисков масив за нуждите на сървърната виртуализация
4.2.	Форм фактор, задължително	За монтаж в 19“ шкаф
4.3.	Контролери, минимум	Резервирани контролери за управление/ 48 GB обща кеш памет
4.4.	Допълнителна кеш памет	Да има възможност за разширение на кеш паметта чрез Flash дискове, масивът да бъде инсталиран с 800 GB допълнителна използваема кеш памет
4.5.	Поддържани видове дискове, задължително	SAS, NL-SAS и SSD едновременно в една система Поддръжка на 3.5“ и 2.5“ дискове едновременно в една система.
4.6.	Максимален брой дискове, минимум	Възможност за разширение до 150 диска
4.7.	Дискови интерфейси, минимум	12 Gbps SAS, резервирани

№	Описание / параметър / компонент	Изискване
4.8.	Подмяна по време на работа	Възможност за подмяна на дисковете по време на работа
4.9.	Използваем капацитет, дискове, минимум	24 TiB, реализирани с 1.2 TB SAS 10K дискове (или с дискове с по-малък капацитет) + 2 диска за защита при отпадане (Hot Spare)
4.10.	Използваем капацитет, дискове, минимум	42 TiB, реализирани с 4 TB NL-SAS 7200 дискове (или с дискове с по-малък капацитет) + 1 диск за защита при отпадане (Hot Spare)
4.11.	Функционалност, задължително	Да включва лиценз за автоматично разпределение на данните между бързи и бавни дискове, в зависимост на натоварването (Automatic Tiering)
4.12.	Функционалност, задължително	Поддръжка на Thin Provisioning Поддръжка на Snapshots
4.13.	Услуги и протоколи, задължително	Поддръжка на файлови услуги – NFS(3,4,4.1), SMB(1,2,3), FTP Поддръжка на блокови услуги – FC, iSCSI
4.14.	Свързаност, минимум	4 броя 10 GbaseT 4 броя 16 Gbps FC
4.15.	Управление, задължително	Да предоставя управление посредством GUI (графичен интерфейс) Да предоставя управление посредством CLI (команден ред)
4.16.	Допълнителни кабели и модули, задължително	Да се достави със всички кабели за свързването му към инфраструктурата
4.17.	Гаранция – минимум, реакция – максимум	3 години от производителя, с поддръжка 24x7 и време за реакция до 4 часа
5.	**Дисков масив тип 3 – 1 брой**	
5.1.	Общо описание, производител, модел	Да се предостави дисков масив за нуждите на софтуера за резервни копия
5.2.	Форм фактор, задължително	За монтаж в 19“ шкаф
5.3.	Контролери, минимум	Резервирани контролери за управление/ 48 GB обща кеш памет
5.4.	Допълнителна кеш памет	Да има възможност за разширение на кеш паметта чрез Flash дискове, масивът да бъде инсталиран с 400 GB допълнителна използваема кеш памет
5.5.	Поддържани видове дискове, задължително	SAS, NL-SAS и SSD едновременно в една система Поддръжка на 3.5“ и 2.5“ дискове едновременно в една система.
5.6.	Максимален брой дискове, минимум	Възможност за разширение до 150 диска
5.7.	Дискови интерфейси, минимум	12 Gbps SAS, резервирани
5.8.	Подмяна по време на работа	Възможност за подмяна на дисковете по време на работа
5.9.	Използваем капацитет, дискове, минимум	85 TiB, реализирани с 4 TB NL-SAS 7200 дискове (или с дискове с по-малък капацитет) + 2 диска за защита при отпадане (Hot Spare)

№	Описание / параметър / компонент	Изискване
5.10.	Функционалност, задължително	Поддръжка на Thin Provisioning Поддръжка на Snapshots
5.11.	Услуги и протоколи, задължително	Поддръжка на файлови услуги – NFS(3,4,4.1), SMB(1,2,3), FTP Поддръжка на блокови услуги – FC, iSCSI
5.12.	Свързаност, минимум	4 броя 10 GbaseT 4 броя 16 Gbps FC
5.13.	Управление, задължително	Да предоставя управление посредством GUI (графичен интерфейс) Да предоставя управление посредством CLI (команден ред)
5.14.	Допълнителни кабели и модули, задължително	Да се достави със всички кабели за свързването му към инфраструктурата
5.15.	Гаранция – минимум, реакция – максимум	3 години от производителя, с поддръжка 24x7 и време за реакция до 4 часа
6.	**Софтуер за сървърна виртуализация**	
6.1.	Общо описание, производител, модел	Да се доставят лицензи за софтуер за виртуализация на 8 бр. сървъри тип 2 с лиценз за общо централизирано управление.
6.2.	Виртуализация, задължително	Пълна виртуализация на паметта, процесорите, логическите дискове и мрежовите адаптери
6.3.	Хардуерна виртуализация, минимум	Поддръжка на технологии за хардуерна виртуализация, като AMD-B, Intel VT
6.4.	Функционалност, задължително	Да няма ограничени в броя на виртуалните машини работещи върху виртуализираните сървъри.
6.5.	Функционалност, задължително	Да подържа 64-битови гост-операционни системи
6.6.	Функционалност, задължително	Поддръжка на Boot from SAN за хипервайзъра
6.7.	Функционалност, задължително	Да може да премества виртуални машини от един физически хост към друг в реално време, без прекъсване на работата и.
6.8.	Функционалност, задължително	Автоматично стартиране на виртуална машина на нов хост в случай на хардуерен проблем.
6.9.	Функционалност, задължително	Да може да се добавя CPU, RAM, HDD, мрежов адаптер към виртуалната машина в реално време, без прекъсване на работата и.
6.10.	Функционалност, задължително	Възможност за динамично разпределение на натоварването, чрез автоматично разпределение на работата на виртуалните машини върху виртуалните хостове.
6.11.	Функционалност, задължително	Система за автоматично динамично управление на разпределението на физическите ресурси между виртуалните машини, способна в реално време да заделя необходимите ресурси за виртуални машини, по предварително зададени правила

№	Описание / параметър / компонент	Изискване
6.12.	Функционалност, задължително	Възможност за оптимизирана консумацията на електроенергия на виртуалната инфраструктура, чрез консолидиране на работещите виртуални машини върху по-малък брой хостове и спирането на освободените хостове
6.13.	Функционалност, задължително	Динамично балансиране на дисковото пространство чрез следене на натоварването на дисковите системи.
6.14.	Функционалност, задължително	Директно презентиране на логически дялове (LUN) от хост средата към виртуалните машини.
6.15.	Функционалност, задължително	Възможност за ограничаване на трафика на мрежовите интерфейси на всяка виртуална машина.
6.16.	Функционалност, задължително	Възможност за създаване и управление на виртуален мрежов комутатор, който обхваща всички сървъри за виртуализация в клъстера.
6.17.	Функционалност, задължително	Възможност за инсталация на хипервайзора върху USB у-ва, SD карти и т.н преносими у-ва.
6.18.	Функционалност, задължително	Да поддържа управление и наблюдение на виртуалните машини и цялостната платформа чрез web клиент
6.19.	Поддръжка, минимум	3 години от производителя, с включени подновявания до по-нови версии и поддръжка в работно време.
7.	**Софтуер за създаване и управление на резервни копия (Backup/Restore)**	
7.1.	Общо описание, производител, модел	Да се достави софтуер за създаване и управление на резервни копия.
7.2.	Лицензи, минимум	Да се достави лиценз за защита на всички виртуални машини (без ограничение на броя им) работещи на специфицираните виртуализирани сървъри тип 1 и 2. Софтуера да поддържа предложената виртуализация в предходната точка, както и Oracle VM
7.3.	Лицензи, минимум	Да се достави допълнителен лиценз за интегрирана защита на Oracle, Microsoft SQL, Informix, MySQL, с големина на данните 2 TB.
7.4.	Функционалност, задължително	Да поддържа глобална дедупликация на данните.
7.5.	Функционалност, задължително	Да не изисква инсталиране на допълнителен софтуер върху виртуалните машини („agentless“) за защитата им.
7.6.	Функционалност, задължително	Възможност за възстановяване на единични обекти/файлове от резервно копие (без допълнително инсталиране на софтуер върху виртуалните машини).

№	Описание / параметър / компонент	Изискване
7.7.	Функционалност, задължително	Възможност за репликиране на резервни копия в резервен център за данни
7.8.	Функционалност, задължително	Пълна поддръжка на лентови библиотеки и виртуални лентови библиотеки.
7.9.	Функционалност, задължително	Възможност за автоматично откриване на нови виртуални машини и прибавянето им към backup задачите.
7.10.	Функционалност, задължително	Възможност за временно стартиране на виртуална машина директно от запазеното копие
7.11.	Функционалност, задължително	Пълна поддръжка и защита на Oracle, Oracle RAC, Oracle ASM и Oracle Data Guard инфраструктури - интеграция с RMAN. Възможност за възстановяване на отделни таблици и бази.
7.12.	Функционалност, задължително	Пълна поддръжка и защита на MS Sql, Informix и MySql, с възможност за извършване на цялостно копие или на копие на отделни бази.
7.13.	Функционалност, задължително	Възможност за създаване на отчети (reports).
7.14.	Функционалност, задължително	Табла за наблюдение на производителност и състоянието на системата.
7.15.	Функционалност, задължително	Управление на всички функционалности през единична централизирана конзола.
7.16.	Поддръжка	3 години от производителя, с включени подновявания до по-нови версии и поддръжка в работно време.
8.	**Мрежови комутатор – 1 брой**	
8.1.	Общо описание, производител, модел	Да се достави L2 мрежови комутатор
8.2.	Интерфейси, минимум	Да бъде оборудван с: 48 броя 10/100/1000 RJ45 ethernet порта (медни) 4 броя 1GE SFP слота за uplink
8.3.	Хардуер, минимум	512MB DRAM 128 MB Flash памет
8.4.	Производителност, минимум	216 Gbps комутираща матрица 107 Mpps ниво на предаване на данни 16000 MAC адреса 9198 байта MTU за L3 пакет за гигабит етернет портовете
8.5.	Функционалност, задължително	Автоматично активиране на порт, който е бил деактивиран поради грешка в мрежата
8.6.	Функционалност, задължително	Да поддържа TFTP и NTP протоколи
8.7.	Функционалност, задължително	Да поддържа следните механизми за превенция на цикли в мрежата: 802.1s, 802.1d или еквивалентни
8.8.	Функционалност, задължително	Проследяване на Layer 2 маршрут
8.9.	Функционалност, задължително	Да поддържа LACP Link Aggregation Control Protocol
8.10.	Функционалност, задължително	Да поддържа минимум 4096 VLAN идентификационни номера

№	Описание / параметър / компонент	Изискване
8.11.	Функционалност, минимум	Да поддържа 1023 активни VLAN
8.12.	Функционалност, задължително	Да поддържа технология за отдалечено наблюдение, анализиране и управление на трафика.
8.13.	Функционалност, задължително	Да поддържа 802.1p class of service (CoS)
8.14.	Функционалност, задължително	Да поддържа класификация на базата на source и destination IP адреси, MAC адреси или Layer 4 Transmission Control Protocol/User Datagram Protocol (TCP/UDP) номера на портове
8.15.	Функционалност, задължително	Минимум 8 изходящи опашки за порт
8.16.	Функционалност, задължително	Да поддържа DSCP класифициране
8.17.	Функционалност, задължително	Да поддържа автоматично осигуряване на качество на услугите включващо класифициране на трафика и конфигурация на изходящите опашки на всеки порт
8.18.	Функционалност, задължително	Да поддържа динамично присъединяване на VLAN към потребител независимо от това къде е свързан потребителя
8.19.	Функционалност, задължително	Да позволява прилагането на политики за сигурност за всеки отделен порт на комутатора
8.20.	Функционалност, задължително	Да поддържа технология за отдалечен достъп посредством SSH протокол
8.21.	Функционалност, задължително	Да поддържа SNMP v1, v2, v3
8.22.	Функционалност, задължително	Да поддържа технология предоставяща AAA-RADIUS, TACACS+ или еквивалентни
8.23.	Функционалност, задължително	ДА поддържа DHCP snooping
8.24.	Функционалност, задължително	Да предотвратява възможността крайни устройства, които не са част от администрираната мрежа да приемат ролята на Spanning-Tree root комутатори.
8.25.	Функционалност, задължително	Да поддържа поне 625 IPv4 Security ACE записа и 500 IPv4 QoS ACE записа
8.26.	Стандарти и сертификати, задължително	UL 60950-1, второ издание
8.27.	Стандарти и сертификати, задължително	CAN/CSA-C22.2 No. 60950-1, второ издание
8.28.	Стандарти и сертификати, задължително	EN 60950-1, второ издание
8.29.	Стандарти и сертификати, задължително	IEC 60950-1, второ издание
8.30.	Стандарти и сертификати, задължително	AS/NZS 60950-1
8.31.	Стандарти и сертификати, задължително	47CFR част 15 клас А
8.32.	Стандарти и сертификати, задължително	EN55022 клас А

№	Описание / параметър / компонент	Изискване
8.33.	Стандарти и сертификати, задължително	ICES003 клас A
8.34.	Стандарти и сертификати, задължително	VCCI клас A
8.35.	Стандарти и сертификати, задължително	CNS13438 клас A
8.36.	Стандарти и сертификати, задължително	EN61000-3-2
8.37.	Стандарти и сертификати, задължително	EN61000-3-3
8.38.	Стандарти и сертификати, задължително	KN22 клас A
8.39.	Стандарти и сертификати, задължително	EN55024
8.40.	Стандарти и сертификати, задължително	CISPR24
8.41.	Стандарти и сертификати, задължително	EN300386
8.42.	Стандарти и сертификати, задължително	KN24
8.43.	Стандарти и сертификати, задължително	Reduction of Hazardous Substances (ROHS) включващ директива 2011/65/EU
8.44.	Управление, задължително	Възможност за достъп до команден интерфейс за управление чрез конзола/telnet/ssh
8.45.	Окомплектовка	Да бъде окомплектован с необходимите монтажни елементи за монтаж в 19” комуникационен шкаф, максимална височина 1 RU
8.46.	Гаранция – минимум, реакция – максимум	3 години от производителя, с поддръжка в работно време и време за реакция до 4 часа.
9.	**Мрежов оптичен преобразовател – 2 броя**	
9.1.	Общо описание, производител, модел	1000BASE-LX/LH оптичен преобразувател за разстояния до 10 км
10.	**Система за мрежова сигурност за идентифициране на потребителите и крайните устройства в мрежата, и управление на достъпа – 1 брой**	
10.1.	Общо описание, производител, модел, продуктов номер	Резервирана система за мрежова сигурност за идентифициране на потребителите и крайните устройства в мрежата, и управление на достъпа
10.2.	Брой поддържани крайни точки, минимум	Системата да включва лиценз за управление на минимум 1000 броя крайни устройства
10.3.	Управление на мрежови устройства	Системата да включва лиценз за администрация и контрол на мрежови устройства
10.4.	Операционна система	Системата да включва операционна система и база данни, за които не е необходим допълнителен лиценз

№	Описание / параметър / компонент	Изискване
10.5.	Виртуализация	Системата да включва лицензи за инсталация на минимум 2 виртуални машини, ако такива са необходими
10.6.	Архитектура	Системата да има разпределена архитектура с цел по-висока надеждност и по-голяма производителност, която да отделя административните и мониторинг функционалности от контролните такива.
10.7.	AAA	Системата да поддържа автентификация, оторизация и отчетност (AAA) на мрежови устройства
10.8.	Интеграция	Системата да има възможност за интеграция с SIEM системи
10.9.	Стандарти	Системата да поддържа RADIUS и 802.1x стандарти
10.10.	IPv6 поддръжка	Системата да поддържа IPv6 крайни точки
10.11.	Функционалности	• контрол на достъпа до мрежата чрез AAA и IEEE-802.1X • управление на guest потребители • криптиране на връзките чрез между потребителите и мрежовите устройства чрез • 802.1AE (MACSec) • API интерфейс
10.12.	Web управление	Системата да поддържа централизиран уеб интерфейс за управление
10.13.	CLI интерфейс	Системата да поддържа Command Line Interface (CLI)
10.14.	Интеграция	Системата да поддържа интеграция с: • Microsoft Active Directory • Lightweight Directory Access Protocol (LDAP) • RADIUS • Системи за идентификация с еднократна парола • Да поддръжка на Open Database Connectivity (ODBC).
10.15.	RADIUS поддръжка	Системата да поддържа RADIUS протокол за удостоверяване, оторизация и отчетност (AAA)

№	Описание / параметър / компонент	Изискване
10.16.	Протоколи	Поддръжка на следните протоколи: • PAP • MS-CHAP • Extensible Authentication Protocol (EAP)-MD5 • Protected EAP (PEAP) • EAP-Flexible Authentication via Secure Tunneling (FAST) • EAP- Transport Layer Security (TLS) • EAP-Tunneled Transport Layer Security (TTLS)
10.17.	TACACS+ поддръжка	Поддръжка на TACACS+ за извършване на автентикация и оторизация на потребители при осъществяването на достъп до устройства, които поддържат TACACS+
10.18.	Потребителски достъп до мрежови устройства	Поддръжка на осигуряване на нива на достъп до определени команди в мрежовите устройства за различни потребители и групи
10.19.	Контрол на достъпа	Системата да предоставя широк набор от опции за контрол на достъпа: • динамично зареждани в мрежовите устройства списъци за контрол на достъпа • динамично назначаване на VLAN-и към потребителите • URL пренасочвания на потребителите • именуване на локално конфигурирани в мрежовите устройства списъци за контрол на достъпа • групи за сигурност с различни тагове
10.20.	Guest функционалност	Системата да поддържа вградени методи за идентификация и обслужване на guest потребители в мрежата, като: • web портал за идентификация на guest потребители • web портал за идентификация на guest потребители, управлявани от специално оторизирани потребители, които не са част от организацията (sponsors)
10.21.	Бъдещо разширение	Да има възможност за добавяне на функционалност позволяваща профилиране на крайни устройства, които се свързват към мрежовата инфраструктура
10.22.	Гаранция	3 години от производителя, с включени подновявания до по-нови версии и поддръжка в работно време.

Забележка: Навсякъде в таблицата, всяко посочване на стандарт, следва да се чете допълнено с думите „или еквивалент“.

Предлаганото от участниците оборудване следва да е ново и неупотребявано.

4. Изисквания за изпълнение на поръчката

4.1. Управление на проекта, включително график за изпълнение

В своето техническо предложение Участникът трябва да предложи методология за управление на проекта, която смята да приложи, като се изтъкнат ползите ѝ за успешното изпълнение на проекта. Предложената методология трябва да съответства на най-добрите световни практики и препоръки (например Project Management Body of Knowledge (PMBOK) Guide, PRINCE2, Agile/SCRUM/Kanban, RUP и др.).

Дейностите по управление на проекта трябва да включват като минимум управление на реализацията на всички дейности и постигане на очакваните резултати, както и разпределението на предложените участници в екипа по роли, график и дейности.

Управление на проекта трябва да осигури:

- координиране на дейностите на експертите от страна на Изпълнителя и Възложителя;
- оптимално използване на ресурсите;
- текущ контрол по изпълнението на дейностите;
- своевременно разпространение на необходимата информация до всички участници;
- идентифициране на промени и осигуряване на анализа и координацията им;
- осигуряване на качеството и полагане на усилия за непрекъснато подобряване на работата за удовлетворяване на изискванията на Възложителя.

Методологията трябва да включва подробно описание на:

- фазите на проекта;
- организация на изпълнение:
  - структура на екипа на Изпълнителя;
  - начин на взаимодействие между членовете на екипа на Изпълнителя;
  - връзки за взаимодействие с екипа на Възложителя;
- проектна документация:
  - видове доклади;
  - техническа и експлоатационна документация;
  - време на предаване;
  - съдържание на документите;
  - управление на версиите;
- управление на качеството;
- график за изпълнение на проекта.

В графика Участникът трябва да опише дейностите и стъпките за тяхното изпълнение максимално детайлно, като покажат логическата връзка между тях. В графика трябва да са посочени датите за предаване на всеки от изготвяните документи.

4.2. Подход за управление на рисковете

В своето техническото предложение Участникът трябва да опише подхода за управление на риска, който ще прилага при изпълнението на проекта.

Участникът трябва да представи и списък с идентифицираните от Възложителя рискове с оценка на вероятност и въздействие и мерки за реакция.

През времето за изпълнение на проекта Изпълнителят трябва да следи рисковете, да оценява тяхното влияние, да анализира ситуацията и да идентифицира (евентуално) нови рискове.

В хода на изпълнение на проекта Изпълнителят следва да поддържа актуален списък с рисковете.

При изготвянето на списъка с рискове Участникът следва да вземе предвид следните идентифицирани от Възложителя рискове:

- външни фактори, водещи до промяна на ключови компоненти на решението и услугите – предмет на настоящата спецификация;
- недобра комуникация между екипите на Възложителя и Изпълнителя при изпълнението на проекта;
- ненавременно изпълнение на всяко от задълженията от страна на Изпълнителя;
- неправилно и неефективно разпределяне на ресурсите и отговорностите при изпълнението на проекта;
- забавяне при изпълнение на проектните дейности, опасност от неспазване на срока за изпълнение на проекта;
- грешки при реализирането на интеграцията;
- липса на задълбоченост при анализа на текущото състояние;
- не информиране на Възложителя за всички потенциални проблеми, които биха могли да възникнат в хода на изпълнение на дейностите;
- риск при поддръжка на оборудването в периода на гаранционна поддръжка.

4.3. Подробно описание на средствата за осигуряване на контрол на качеството

В своето Техническо предложение, Участникът трябва да предостави подробно описание на средствата за осигуряване на качеството, които смята да използва по време на изпълнение на проекта. Участникът трябва да опише процедурите за осигуряване на качеството и контрол, които ще приложи при изпълнение на проекта – описание на основните процеси и стъпки по осигуряване на качеството и контрола с цел постигане на качествено изпълнение на проекта.

4.4. Концептуален проект

В техническото предложение Участникът следва да предостави „Концептуален проект“, който да съдържа следните елементи:

- Техническо предложение за виртуална инфраструктура – дискови масиви за виртуална инфраструктура, сървъри, софтуер за виртуализация на 8 броя „сървъри тип 2“, Oracle VM софтуер за виртуализация на 2 броя „сървъри тип 1“, включващо:
  - представена архитектура на решението, подкрепена с описание на основните използвани технологии, компоненти, физическа и логическа топология, организация на дисковото пространство, използвани функционалности на сървърните виртуализации;
  - представена реализация на резервираност, която е подкрепена с примери и/или сценарии;
  - представена аргументация за концептуалното решение, включваща примери, графики, сравнения с други решения, алтернативни подходи, плюсове и минуси на алтернативите;

- представен сценарий за тестване, който включва описание на дейностите, използвани методи, основни етапи, извършвани тестове и критерии за оценка.

- Техническото предложение за система за създаване и управление на резервни копия, включващо:
  - представена архитектурата на решението, подкрепена с описание на основни използвани технологии, компоненти, физическа и логическа топология, предложение за реализация на автоматичните задачи за резервни копия, организация на дисковото пространство за резервни копия, използвани функционалности;
  - представена аргументация за концептуалното решение, която включва в себе си примери, графики, сравнения с други решения, алтернативни подходи, плюсове, минуси на алтернативите;
  - представен сценарий за тестване, който включва описание на дейностите, използвани методи, основни етапи, извършвани тестове и критерии за оценка.
- Техническото предложение за системата за мрежова сигурност, включващо:
  - представена архитектура на решението, подкрепена с описание на основните използвани технологии и компоненти, физическа и логическа топология, примерни конфигурации на мрежовите устройства;
  - представена реализацията на резервираността, подкрепена с примери и /или сценарии;
  - представена аргументация за концептуалното решение, която включва в себе си примери, графики, сравнения с други решения, алтернативни подходи, плюсове, минуси на алтернативите;
  - представени политики за сигурност, включващи цели и ползи, както и въздействие върху работата на системите и потребителите;
  - представен сценарий за тестване, който включва описание на дейностите, използвани методи, основни етапи, извършвани тестове и критерии за оценка.

4.5. Обучение

Изпълнителят след приключване на услугите по въвеждане в експлоатация на хардуерното, комуникационното оборудване и софтуерните решения следва да проведе обучение на посочени от Възложителя служители за работа с функционалните възможности на:

- софтуер за сървърна виртуализация;
- софтуер за създаване и управление на резервни копия (Backup/Restore);
- система за мрежова сигурност за идентифициране на потребителите и крайните устройства в мрежата, и управление на достъпа.

4.6. Специфични изисквания за сигурност

При необходимост от ремонт или подмяна на оборудване се връщат само компоненти, които не съдържат постоянна или временна памет, която може да съдържа чувствителна информация. При фабрично заложена възможност за демонтиране на такава памет без допълнителни инструменти (FLASH памет, EEPROM, твърд диск, RAM памет) същите се демонтират от компонента преди да бъде предаден на Изпълнителя за ремонт или подмяна. Компоненти, при които не съществува такава възможност, не се връщат на доставчика за ремонт или подмяна, а се унищожават. Унищожаването се извършва от Възложителя, в присъствие на представител на Изпълнителя, за което се изготвя двустранен протокол, а Изпълнителя заменя унищожения компонент с нов.

4.7. Участникът трябва да притежава и прилага сертифицирана система за управление на сигурността на информацията, съответстваща на стандарт БДС EN ISO/IEC 27001:2014 или еквивалентен.

Сертификатът трябва да е валиден и да е издаден от независими лица, които са акредитирани по съответната серия европейски стандарти от Изпълнителна агенция „Българска служба за акредитация“ или от друг национален орган по акредитация, който е страна по Многостранното споразумение за взаимно признаване на Европейската организация за акредитация, за съответната област или да отговарят на изискванията за признаване съгласно чл. 5а, ал. 2 от Закона за националната акредитация на органи за оценяване на съответствието. Възложителят приема еквивалентни сертификати, издадени от органи, установени в други държави членки. Когато участникът не е имал достъп до такъв сертификат или е нямал възможност да го получи в съответните срокове по независещи от него причини, той може да представи други доказателства за еквивалентни мерки за осигуряване на система за управление на качеството. В тези случаи участникът трябва да е в състояние да докаже, че предлаганите мерки са еквивалентни на изискваните.

4.8. Участникът трябва да притежава и прилага сертифицирана система за управление на ИТ услуги, съответстваща на стандарт БДС EN ISO/IEC 20000-1:2012 или еквивалентен.

Сертификатът трябва да е валиден и да е издаден от независими лица, които са акредитирани по съответната серия европейски стандарти от Изпълнителна агенция „Българска служба за акредитация“ или от друг национален орган по акредитация, който е страна по Многостранното споразумение за взаимно признаване на Европейската организация за акредитация, за съответната област или да отговарят на изискванията за признаване съгласно чл. 5а, ал. 2 от Закона за националната акредитация на органи за оценяване на съответствието. Възложителят приема еквивалентни сертификати, издадени от органи, установени в други държави членки. Когато участникът не е имал достъп до такъв сертификат или е нямал възможност да го получи в съответните срокове по независещи от него причини, той може да представи други доказателства за еквивалентни мерки за осигуряване на система за управление на качеството. В тези случаи участникът трябва да е в състояние да докаже, че предлаганите мерки са еквивалентни на изискваните.