EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program

MINISTERSTVO
PRO MÍSTNÍ
ROZVOJ ČR

Příloha č. 1 Specifikace vlastností poptávaného řešení

TECHNICKÁ SPECIFIKACE

pro veřejnou zakázku

„Zajištění dostupnosti a bezpečnosti ICT a rozšíření stávajících IS“

Část A - Hardware

Obsah

1. Výchozí stav IT infrastruktury

Úvodní informace

Oblastní nemocnice Mladá Boleslav, a. s., nemocnice Středočeského kraje (Klaudiánova nemocnice) je zařízení, jehož zakladatelem a jediným akcionářem je Středočeský kraj. Primární službou a důvodem existence nemocnice je poskytování lékařské péče pro více než 200.000 obyvatel severovýchodní části Středočeského kraje. Nemocnice v současné době poskytuje péči prostřednictvím 33 oddělení. Nabízí 582 lůžek a během roku poskytla 1,2 mil. ambulantních vyšetření, 13 tisíc chirurgických zákroků a v průměru hospitalizuje 451 pacientů za den[1].

Současné směrování nemocnice je dáno následující vizí:

- bezpečnost pacientů
- dosažení a udržení akreditace nemocnice
- bezpečnost pacientů
- poskytování zdravotní péče na vysoce odborné a profesionální úrovni
- neustále zvyšovat kvalitu poskytované péče
- nemocnice otevřená, přátelská a dobře komunikující uvnitř a navenek
- nemocnice transparentní a ekonomicky soběstačná

Stav informačních a komunikačních technologií

Výchozí stav v oblasti informačních a komunikačních technologií je popsán na základě informací Odboru informatiky a na základě dokumentu **Analýza nákladů ICT a návrh jejich optimalizace** (strategický dokument pro řízení IT v období 2013 – 2016), verze 1.4 ze dne 13.6.2014.

Odbor IT aktuálně v pěti pracovnících zajišťuje služby správy IT prostředí, které má přibližně 2.000 pracovníků, kteří používají 700 personálních počítačů, používají 22 podnikových aplikací, tisknou na 459 tiskáren, používají 170 IP a digitálních telefonů, vše provozováno v jednom datovém centru s 13 fyzickými a 36 virtuálními servery. Aktuálně je prostředí ve správě IT funkční. V roce 2012 činili celkové náklady na IT 22.043.504 Kč, v porovnání s předchozími lety s rostoucí tendencí. Z toho 35 % těchto nákladů zahrnuje odbor IT (SW, práce, mzdy, odpisy), 27 % jsou provozní výdaje na podnikové aplikace a 13 % platby za pravidelné služby (internet, mobil, pevné linky).

[1] Zdroj: http://www.klaudianovanemocnice.cz/o-nemocnici

1.1 Aplikační část

S ohledem na cíle projektu definované v kapitole **Chyba! Nenalezen zdroj odkazů.** studie jsou níže **popsány nevyhovující oblasti**, ze kterých tyto cíle vzešly:

- **Manažerský informační systém**

  V oblasti manažerských nástrojů pro podporu řízení není v nemocnici aktuálně provozován žádný SW nástroj. V roce 2007 se v rámci nemocnice uvažovalo o pořízení manažerského informačního systému jako nadstavby nad nemocničním IS MEDEA, nicméně k implementaci a zprovoznění manažerského informačního systému a jeho funkcionalit nakonec nedošlo.

  Absenci nástroje MIS zmiňuje i zpracovaná „Analýza nákladů ICT a návrh jejich optimalizace“ z roku 2013, kde je v kvadrantu Slabé stránky hodnotící SWOT analýzy uvedena položka „Zcela chybějící podpora manažerských funkcí pro podporu rozhodování“. Současný stav v oblasti podpory manažerského rozhodování lze vyhodnotit jako nevyhovující.

- **Plánování a řízení operačních sálů**

  V současné době není plně využívána IT podpora k objednávání pacientů na plánované operace, pro optimalizaci časového vytížení operačních sálů, porovnání výkonnosti operatérů nebo sledování vývoje jednotlivých druhů nákladů v čase a v závislosti na druhu operace. Absentuje zaznamenání akcí provedených během operace, nejsou k dispozici výstupy v podobě perioperačního záznamu s možností generování objednávek pro doplnění použitého materiálu.

- **Evidence a řízení nástrojů pro operace**

  V současné době není plně využívána IT podpora pro evidenci nástrojů v nemocnici, jejich použití a opravy. Z toho vyplývají složité postupy pro určení nákladů v čase a v závislosti na druhu operace. S ohledem na ruční faktor zde je i přímá vazba na chybovost (zcela zásadní faktor), snížení nákladů a zajištění úspory času zaměstnanců v oblasti přípravy nástrojů pro operace.

1.2 Technologická a infrastrukturní část

Společným jmenovatelem všech výše uvedených oblastí je **infrastruktura. Odbor IT uvažoval progresivně a v minulých letech virtualizoval servery na platformě VMware vSphere. Virtualizovány jsou všechny servery, kde to bylo prakticky možné. Fyzické servery jsou nyní pouze ty, které technologicky nelze virtualizovat (MEDEA) nebo je fyzické oddělení podmíněno funkčností (firewall, monitoring, backup). Ze slabých stránek současného stavu infrastruktury lze zmínit dva body:**

- **není nastaven jednotný princip životního cyklu zařízení (doba obnovování podle kategorie zařízení)**

- **není důsledně používán princip odstraňování Single Point of Failure pro zajištění dostupnosti infrastruktury jako celku**

Serverová infrastruktura je umístěna ve dvou oddělených datových centrech (serverovnách) v budově nemocnice. Datová centra nejsou plně schopna vzájemně převzít své role (resp. část rolí) v případě poruchy jednoho z nich.

Datové centrum 1 „v budově nové Interny – 1.NP“ je primární, je v něm umístěna většina technologií. Datové centrum 2 „v budově Interny – 1.NP“ slouží jako sekundární.

Zálohování virtuálních serverů je řešeno centrálně. Zálohy jsou systémem Veeam Backup & Replication a Backup Exec ukládány na samostatný server.

Pro překlenutí krátkodobých výpadků elektrické energie jsou datová centra vybavena záložními zdroji UPS, při delších výpadcích zajišťuje dodávku elektrické energie automaticky spouštěný motorgenerátor. Všechna datová centra jsou vybavena standardními podpůrnými (non-IT) systémy zajišťujícím provoz serverové infrastruktury – klimatizace, monitorovací systémy

Architektura serverové infrastruktury využívá výhod virtualizačních technologií ve všech klíčových vrstvách.

Současný stav infrastruktury neumožňuje rozšiřování počtu aplikací, informačních systémů a databázových systémů pro nedostatek výkonu a kapacity. V rámci realizace projektu je proto navrženo komplexní řešení, jehož cílem bude systematické doplnění stávající infrastruktury organizace, které umožní řádný provoz nově nasazovaných aplikací a informačních systémů a zároveň které bude možné vhodně sloučit s infrastrukturou stávající. Pro možnost řádného fungování a možnosti nasazení v projektu realizovaných aktivit bude nezbytné respektovat současný stav infrastruktury organizace a tu vhodným způsobem o potřebné prostředky doplnit a odpovídajícím způsobem v potřebných částech povýšit, např. konkrétně síťová infrastruktura musí být odpovídajícím způsobem připravena na vyšší datové toky způsobené nasazením nových aplikací a infomačních systémů.

2. Požadavky na dodávku, implementaci a zpracování nabídky

Předmětem této veřejné zakázky je dodávka „Zajištění dostupnosti a bezpečnosti ICT a rozšíření stávajících IS“ na základě Studie proveditelnosti zadavatele a to pro část A – Hardware, která zahrnuje následující oblasti Infrastruktury:

- Bezpečnost sítě – NGFW Firewall
- Podpůrná infrastruktura – Server vč. operačního systému a diskové pole

Požadavky na implementaci

Dodávka a implementace systémů bude součástí plnění dodavatele vybraného v rámci veřejné zakázky. V této zadávací dokumentaci je uveden seznam minimálních požadovaných

parametrů a definovaného rozsahu implementačních prací. Před vlastní implementací vznikne ve spolupráci dodavatele a zadavatele cílový koncept, kde bude popsán konkrétní způsob a rozsah integrace a implementované postupy.

Informační systém v rámci stávající infrastruktury zadavatele bude využívat existující mechanismy a zálohovací infrastrukturu.

V rámci implementace řešení bude dodavatelem provedena integrace na identity management systém zadavatele tak, aby mohly být užívány existující identity uživatelů bez nutnosti zakládání nových pro daný informační systém. Odpovídající rozhraní s popisem struktury informace pro napojení na odpovídající identity management systém bude poskytnuto dodavatelům na základě jejich žádosti zadavateli.

Požadavky na školení

Školení zaměstnanců zadavatele bude součástí dodávky, implementace a nasazování systémů do provozu a bude provedeno v takovém rozsahu, aby pracovníci zadavatele byli schopni systém rutinně obsluhovat a systém užívat.

Požadavky na dokumentaci

Součástí plnění bude také poskytnutí dokumentace pro používání dodávaných zařízení a informačního systému, provádění jednotlivých nastavení, včetně příkladů typových úloh min. v rozsahu užívání základních funkcionalit.

Požadavky na technickou podporu

Předpokladem je, že rutinní provoz budou zajišťovat stávající zaměstnanci odboru informatiky zadavatele. Většina nově dodávaných systémů je technologicky složitá a zadavatel nemá k dispozici odpovídající kvalifikované pracovníky pro zajištění technické podpory v nestandardních situacích (porucha, výpadek, nestabilita apod.). Zároveň je technická podpora klíčovým faktorem úspěšnosti nasazení a provozování těchto produktů v horizontu doby udržitelnosti projektu, proto bude technická podpora zajištěna současně s pořízením nových technologií, tzn. dodavatelsky.

Požadavky na zpracování nabídky

Uchazeč jako součást nabídky předloží popis navrhovaného řešení, které splňuje veškeré požadavky zadavatele uvedené v této zadávací dokumentaci a studii proveditelnosti.

Tabulka splnění minimálních požadavků na soulad nabídky dodávaného řešení a služeb se zadávací dokumentací a studií proveditelnosti		
Požadavky na dodávku a implementaci včetně funkcionalit		**Splňuje (Ano/Ne)**
1	Účastník potvrzuje soulad předložené nabídky dodávaného řešení a služeb se zadávací dokumentací a studií proveditelnosti.	**ANO**

3. Vymezení rozsahu veřejné zakázky

3.1 Část I. – Infrastruktura

- HW firewally
- HW serverová infrastruktura včetně OS
- HW diskové pole včetně SW

3.1.1 Minimální požadavky na HW firewally

Popis požadované funkcionality

Nově nasazený NGFW firewall zajistí ochranu vnitřní sítě (a všech prostředků dostupných ve vnitřní síti) od sítí mimo organizaci. Zároveň umožní zamezit nežádoucím aktivitám v odchozím směru z nemocniční sítě. Firewall doplní současnou infrastrukturu o potřebné bezpečnostní systémy tak, aby organizace vyhověla základním požadavkům kladeným zákonem číslo 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

Vysoce dostupný firewallový cluster bude tvořený dvěma hardwarovými firewally zapojenými do celku, který vykazuje vysokou dostupnost - v případě výpadku/ poruchy jednoho firewallu přebere druhý firewall automaticky všechny síťové úlohy. Zařízení samotné pak bude spojovat funkce firewallu, antiviru a antispamu, IDS, řízení provozu, filtrování webového obsahu.

Požadavky na vlastnosti řešení:

- Integrovaný antivirus bude odhalovat a odstraňovat viry, červy a spyware v reálném čase. Bude prohlížet přílohy příchozích a odchozích emailů (SMTP, POP3, IMAP) a veškerý provoz přes FTP a HTTP včetně webových emailů. Antivirové gateway bude nasazena s cílem zastavit viry a červy ještě před vniknutím do sítě.
- Firewall bude zastavovat útoky, které obcházejí běžné host-based antivirové systémy, přičemž musí reagovat v reálném čase na rychle se šířící útoky.
- Zařízení poskytne podporu VPN standardů IPSec, PPTP a L2TP a umožní bezpečnou komunikaci mezi sítí a klienty a ověří uživatele, zašifruje data a spravuje relace. Takové VPN umožní komunikaci na vysoké úrovni zabezpečení, která s ohledem na převážnou citlivost informací zpracovávaných v organizaci je v této oblasti prioritou. Nově nasazený informační systém totiž umožní v rámci sestavování virtuálních privátních sítí použit nejnovější metody a nejrobustnější formy šifrování. To je důležité zejména s ohledem na skutečnost, že za poslední dekádu bylo odhaleno mnoho exploitů stávajících řešení šifrované komunikace, a na základě těchto zjištění bylo potřeba zajistit povýšení standardů v této oblasti. Pro možnost zajištění odpovídající zabezpečené komunikace umožňující interoperabilitu informačních systémů provozovaných organizací bude povýšení takového informačního systému nezbytné.

- Integrovaný antispam bude udržovat seznamy zakázaných (black list) a povolených (white list) domén, IP adres a emailových adres, které mohou být spravovány a aktualizovány podle jednotlivých uživatelů nebo pro celý úřad. Součástí technologie bude mj. Bayesian algoritmus, který je možné personalizovat pro každého uživatele a přizpůsoben automaticky změnám ve spamu
    - Bayesianská analýza srovnává slova nebo fráze v emailu s ohledem na četnost stejného slova nebo frází v předchozích emailech příjemců (jak legitimních, tak spamů).
    - Obsahová filtrace koordinuje činnost s URL filtrací - jde o techniku otisků vyhledávající specifické URL obsažené ve zprávách a porovnává je s URL dříve identifikovanými jako původci spamu.
- Zařízení umožní díky profilování provozu kontrolovat síťový provoz za účelem optimalizace nebo garance výkonu, nízké čekací doby a šířky pásma pro danou službu.
- Zařízení umožní třídění paketů, systém řazení ve frontě, prosazování pravidel, regulaci přetížení, kvalitu služby (QoS) a dostupnost. Jelikož šířka pásma je limitovaný zdroj, profilování provozu pomáhá seřadit síťové služby podle důležitosti a prioritizovat je. Racionálně spravované profilování provozu zlepšuje dobu odezvy, dostupnost služby a využití celého pásma bez výpadků způsobených intenzivním multimediálním či peer-to-peer provozem.
- Firewall dále bude testovat veškerý webový obsah na výskyt známých nežádoucích URL, blokuje nevhodný obsah a nebezpečné Java aplety, cookies, Active X skripty před jejich vstupem do sítě. Filtrace budou také uživatelsky přizpůsobitelné, aby umožnily síti organizace přidat další URL pro zabránění přístupu k dalším nežádoucím stránkám.
- SW analyzátor událostí - bude specializovaná aplikace, zaměřená na shromažďování, analýzu, agregaci a korelaci bezpečnostních událostí, která v reálném čase prezentuje informace ze síťové infrastruktury - firewallů.
- Analyzátor událostí bude provádět sběr strojových dat z firewallů a pro ty následně provede korelaci do komplexních událostí.
- Analyzátor událostí bude shromažďovat a katalogizovat logy a data událostí, a to v reálném čase - automaticky sesbírá, setřídí a shromáždí veškeré data v protokolech a na základě těchto informací poskytne real-time zpravodajství.

Bezpečnostní opatření celého technického řešení bude ještě doplněno o anti X software na zařízeních (PC stanice, notebooky, servery...). Koncových zařízení je cca 750, ochrana na stanicích bude umožňovat kromě standardních funkcí jako je AV ochrana také monitoring – kontrola připojené pracovní stanice na patch level, instalovaný vhodný service pack, antivirový software, personální firewall. Zmíněný anti X software není předmětem dodávky NGFW firewallu.

Požadavky na architekturu řešení:

Řešení bude v rámci jednotlivých prvků nasazeno do infrastruktury nemocnice a bude provázáno v rámci své funkcionality. Kritické HW součásti zařízení, které dokáží převzít svoji roli v případě výpadku navzájem, budou v rámci infrastruktury organizace fyzicky umístěny v oddělených a nesousedících prostorech.

Požadavky na integrační vazby:

Není relevantní.

Požadavky na využití infrastruktury zadavatele:

Není relevantní.

Požadavky na dostupnost služby:

Informační systém řízení bezpečnosti síťové komunikace musí být dostupný nepřetržitě, neboť umožňuje řídit a oddělovat datové toky povolené od datových toků zakázaných. Požadavek na dostupnost služby je proto 24/7 s SLA 99,9 %.

Požadavky na NGFW Firewall – HW technické parametry:

Dodávka a implementace vysoce dostupného clusteru složeného ze dvou HW firewallů typu New Generation FireWall – podpora práce s logickými objekty (aplikace, uživatelé, URL adresy, lokality apod.).

Každý firewall musí splňovat následující minimální požadavky:

- Provedení – umístitelné do 19“ racku
- Počet síťových rozhraní LAN 1 Gb – min 20×, z toho min. 2× SFP
- Interní úložiště typu flash pro ukládání logů apod. – min. 50 GB
- Počet rozhraní USB pro připojení ext. modemu – min. 1×
- Výkon Propustnost firewallu min. 3 Gb/s nezávisle na velikosti packetu
- Propustnost firewallu – min. 4 Mpps (pps - paketů za sekundu)
- Počet FW politik min. 10 000
- Počet současných otevřených spojení – min. 3 M
- Propustnost VPN – min. 1 Gbps
- Propustnost IPS – min 1,5 Gbps
- Propustnost antiviru – min. 1 Gbps

Požadavky na záruku a servisní podporu:

Záruka 5 let, servisní podpora 8x5 s odezvou do 24 hodin a opravou do 48 hodin.

Tabulka splnění minimálních požadavků na soulad nabídky dodávaného řešení a služeb se zadávací dokumentací a studií proveditelnosti		
Požadavky na dodávku a implementaci včetně funkcionalit		**Splňuje (Ano/Ne)**
1	Uchazeč potvrzuje soulad nabídky dodávaného řešení s požadavky na dodávku a implementaci NGFW firewallů	**ANO**

3.1.2. Minimální požadavky na HW serverovou infrastrukturu včetně OS

V souvislosti s pořízením nového IS je potřeba zajistit vybudování nezbytné infrastruktury v rámci realizovaného projektu. Další aktivitou je nasazení této nové infrastruktury mezi stávající vybavení organizace, a tyto nové prostředky vhodně implementovat co do jejich fyzického umístění, tak i co do umístění logického. V této souvislosti je tedy i cílem konsolidace a optimalizace prostředků, včetně optimalizace jejich fyzického rozmístění v budovách organizace.

Požadavky na jednotlivé technologie a počty licencí vycházejí z požadavků jednotlivých oblastí IS, který má být pořízen v rámci projektu (*Manažerský informační systém, Plánování a řízení operačních sálů, Evidence a řízení nástrojů pro operace, Bezpečnost sítě – NGFW Firewall*). V rámci popisu technického řešení daných oblastí (podkapitoly v **Chyba! Nenalezen zdroj odkazů.** studie) tedy proběhlo shrnutí požadavků na infrastrukturu – nyní tak lze dimenzovat a specifikovat nezbytně nutný hardware, který má být v souvislosti s realizací projektu pořízen, tak aby umožnil běh informačních systémů.

Požadavky na podpůrnou infrastrukturu – technické parametry:

Dodávka a implementace HW serveru včetně softwaru.

Dodávka licencí SW a instalace:

Serverový operační systém - OEM Win Svr Datacenter 2012 R2 x64 Eng 1pk DVD 2 CPU – 1×

Dodávka a instalace HW:

- SRV 2× 14 jader, včetně interních disků – dodávka HW včetně implementace
  - Procesor 2× min. Intel Xeon 14 jádrový
  - Paměť RAM min. 512 GB DDR4, 2400+ MHz
  - Síťová připojení min. 2 porty 10 Gbit Ethernet SFP+
  - Síťová připojení min. 2 porty 40 Gbit Ethernet QFP+
  - Síťová připojení min. 4 1Gbe ethernet porty
  - Řadič RAID s min. 4GB FBWC cache, kompatibilní řadič pro SSD diskovou technologii
  - HDD min. 16× 500GB SSD SAS
  - Napájecí zdroje - 2x - max. 800W, včetně napájecích kabelů
  - Provedení RACK max. 2U. Součástí dodávky musí být veškerý potřebný materiál pro připevnění serveru do racku.

- Vzdálená správa Součástí serveru musí být integrovaná HW vzdálená správa s funkcí vzdálené konzole bez nutnosti běžícího OS. Systém pro vzdálenou správu musí mít vlastní dedikovaný ethernetový port typu RJ-45.
- HBA 2× FC 16Gb"

Součástí dodávky je i montáž zařízení do 19“ stojanu (racku) a základní konfigurace dle požadavku zákazníka (min. zapojení, oživení, příprava prostředí pro správu diskového pole a aktualizace firmware).

Požadavky na záruku a servisní podporu:

Záruka 5 let, servisní podpora 8x5 s odezvou do 24 hodin a opravou do 48 hodin.

Tabulka splnění minimálních požadavků na soulad nabídky dodávaného řešení a služeb se zadávací dokumentací a studií proveditelnosti		
Požadavky na dodávku a implementaci včetně funkcionalit		**Splňuje (Ano/Ne)**
1	Uchazeč potvrzuje soulad nabídky dodávaného řešení s požadavky na dodávku a implementaci HW serveru včetně OS	**ANO**

3.1.3. Minimální požadavky na HW diskové pole včetně SW

V souvislosti s pořízením nového IS je potřeba zajistit vybudování nezbytné infrastruktury v rámci realizovaného projektu. Další aktivitou je nasazení této nové infrastruktury mezi stávající vybavení organizace, a tyto nové prostředky vhodně implementovat co do jejich fyzického umístění, tak i co do umístění logického. V této souvislosti je tedy i cílem konsolidace a optimalizace prostředků, včetně optimalizace jejich fyzického rozmístění v budovách organizace.

Požadavky na jednotlivé technologie a počty licencí vycházejí z požadavků jednotlivých oblastí IS, který má být pořízen v rámci projektu (*Manažerský informační systém, Plánování a řízení operačních sálů, Evidence a řízení nástrojů pro operace, Bezpečnost sítě – NGFW Firewall*). V rámci popisu technického řešení daných oblastí (podkapitoly v **Chyba! Nenalezen zdroj odkazů.** studie) tedy proběhlo shrnutí požadavků na infrastrukturu – nyní tak lze dimenzovat a specifikovat nezbytně nutný hardware, který má být v souvislosti s realizací projektu pořízen, tak aby umožnil běh informačních systémů.

Požadavky na diskové pole – technické parametry:

Dodávka a implementace ALL Flash HW diskového pole.

- Základní box se dvěma hot-swap redundantními aktivními řadiči, plně odolný proti výpadku klíčových komponent (No Single Point of Failure) včetně řadičů, cache paměti, ventilátorů, napájecích zdrojů.

Každý řadič bude obsahovat:

- nejméně 8 portů FC 16Gbps pro připojení k SAN infrastruktuře, s možností rozšíření portů, vyrovnávací paměť (CACHE) nejméně 32GB
- Min. 30 disků o hrubé diskové kapacitě 120TB, SSD
- Veškeré potřebné kabely pro připojení pole k UPS (C13/C14) a k FC switchům všemi FC porty
- Ližiny pro připevnění diskového pole do racku

Součástí nabídky musí být software a licence (pokud jsou třeba) pro následující funkcionality diskového pole:

- Základní software umožňující správu diskového pole včetně licence pro připojení min. 64 serverů (Windows/Linux/VMware)
- Funkce Call-Home
- Snapshoty a thin provisioning pro celou nabízenou kapacitu diskového pole
- Inline deduplikaci

Součástí dodávky je i montáž zařízení do 19“ stojanu (racku) a základní konfigurace dle požadavku zákazníka (min. zapojení, oživení, příprava prostředí pro správu diskového pole a aktualizace firmware).

Požadavky na záruku a servisní podporu:

Záruka 5 let, servisní podpora 8x5 s odezvou do 24 hodin a opravou do 48 hodin.

Součástí pořizovaného hardware budou současně i softwarové licence nezbytné pro zajištění provozu daného řešení v infrastruktuře organizace a umožňující provoz IS realizovaného v rámci projektu. Součástí pořízení hardware bude současně i požadavek na provedení implementace, na záruku a na technickou podporu.

Tabulka splnění minimálních požadavků na soulad nabídky dodávaného řešení a služeb se zadávací dokumentací a studií proveditelnosti		
Požadavky na dodávku a implementaci včetně funkcionalit		**Splňuje (Ano/Ne)**
1	Uchazeč potvrzuje soulad nabídky dodávaného řešení s požadavky na dodávku a implementaci diskového pole	**ANO**

3.2 Část II. – Servisní podpora

3.2.1 Minimální požadavky na servisní podporu hardware – SLA

Požadovaná servisní podpora na hardware

Zadavatel požaduje v rámci dodávky hardwaru zajištění servisní podpory v režimu 8x5 s odezvou do 24 hodin a opravou do 48 hodin.

3.2.2 Minimální požadavky na záruky

Záruka a servis na systémy budou řešeny servisní smlouvou – ta bude hrazena z vlastních prostředků příjemce dotace. Ta bude zahrnovat minimální rozsah daný technickou podporou a dále výměnu vadného HW minimálně po dobu udržitelnosti projektu. Vyčíslené výdaje na záruku na jakost dodaného plnění jsou způsobilé pouze v období realizace projektu. Část vyčíslených výdajů spadajících do období udržitelnosti je nezpůsobilá. Výdaje na jakýkoli servis jsou nezpůsobilé.

Záruka za jakost znamená závazek prodávajícího, že dodané zboží bude po určitou dobu způsobilé pro použití ke smluvenému, jinak k obvyklému účelu nebo že si zachová smluvené, jinak obvyklé vlastnosti. Záruka za jakost je tedy dobrovolným prohlášením prodávajícího ohledně jakosti jím prodávaného zboží. Převzetí závazku ze záruky může dle Obchodního zákoníku vyplynout ze smlouvy nebo i z pouhého prohlášení prodávajícího, zejména ve formě záručního listu. Účinky převzetí tohoto závazku má i vyznačení délky záruční doby nebo doby trvanlivosti nebo použitelnosti dodaného zboží v akceptačním protokolu.

Požadovaná záruka na hardware, resp. délka záruky na jakost dodaného plnění bude zahrnovat pouze bezplatnou výměnu hardwaru, nebo komponent (včetně ventilátorů či napájecích zdrojů). Záruka se nevztahuje na vady, způsobené běžným opotřebením při používání věci nebo další servis.

Délka minimální požadované záruky je zadavatelem stanovena na 60 měsíců od okamžiku převzetí zboží kupujícím.

Záruka nad rámec výše uvedeného a servis na systémy budou řešeny servisní smlouvou a budou hrazeny z rozpočtu organizace. Ta bude zahrnovat rozsah daný případnou technickou podporou a dále profylaxe, opravy nebo výměny po dobu udržitelnosti projektu nad rámec sjednané záruky za jakost. S ohledem na stávající personální zabezpečení se jako postačující jeví nastavení SLA v režimu 8×5 NBD.

Při průzkumu trhu (indikativních nabídkách) bylo zjištěno, že dodavatelé většinou vyžadují servisní smlouvu zahrnující další technickou podporu SW i HW. Vzhledem k tomu, že se o rutinní provoz a údržbu budou starat zaměstnanci organizace, bude cena údržby a případných oprav nad rámec sjednané záruky za jakost zahrnuta v ceně servisní smlouvy nebo smlouvy o technické podpoře.

Požadované parametry dodané technologie z hlediska životnosti, pravděpodobnosti poruchy a záruky:

Technologie	Životnost (roky)	Pravděpodobnost poruchy (%)	Záruka (roky)
NGFW Firewall	5	2	5
Server 2× 14 jader, včetně interních disků	5	2	5

ALL Flash diskové pole	5	2	5

Tabulka splnění minimálních požadavků na soulad nabídky dodávaného řešení a služeb se zadávací dokumentací a studií proveditelnosti		
Požadavky na dodávku a implementaci včetně funkcionalit		**Splňuje (Ano/Ne)**
1	Uchazeč potvrzuje soulad nabídky dodávaného řešení s požadavky na životnost, pravděpodobnost poruchy a záruky	**ANO**

3.2.3 Minimální požadavky na servisní podporu provozu

Běžná **technická podpora** bude zajišťována pracovníky odboru informatiky, kteří budou pro tuto činnost školeni v rámci implementace a nasazování systémů. Technická podpora pro hardwarové komponenty projektu bude zajišťována výrobcem a pro softwarové komponenty bude zajišťována dodavatelem, na základě uzavřené smlouvy o podpoře provozu, minimálně po dobu udržitelnosti projektu.

Požadovaná podpora provozu bude rozdělena na dvě části:

- podporu provozu ve formě základní podpory tzn. zajištění maintenance a SW aktualizací dle běžných podmínek poskytovaných výrobci. Zajištění základní podpory bude požadováno v rámci dodávek.
- rozšířená podpora – zajistí maintenance a SW aktualizace nad rámec běžných podmínek poskytovaných výrobci – rozšířená podpora bude zajištěna a hrazena z vlastních prostředků příjemce dotace.

Tabulka splnění minimálních požadavků na soulad nabídky dodávaného řešení a služeb se zadávací dokumentací a studií proveditelnosti		
Požadavky na dodávku a implementaci včetně funkcionalit		**Splňuje (Ano/Ne)**
1	Uchazeč potvrzuje soulad nabídky dodávaného řešení s požadavky na servisní podporu provozu	**ANO**