



**Spolufinancováno  
Evropskou unií**



**MINISTERSTVO  
PRO MÍSTNÍ  
ROZVOJ ČR**

## **Příloha 3.c Technická specifikace – Část 2**

### **Technické požadavky na přístupovou infrastrukturu a zálohování**

**k Zadávací dokumentaci projektu „Komplexní ochrana  
celonemocničního informačního systému ONK vůči  
kybernetickým hrozbám“**

## Obsah

1. Zkratky a pojmy .....	3
2. Místo plnění.....	4
3. Doba plnění.....	4
4. Způsob prokázání splnění požadavků minimálního plnění.....	5
5. Požadavky na jednotlivé položky přístupové infrastruktury a zálohování .....	5
6. Fáze A - Instalace a implementace .....	14
7. Fáze B – provozní podpora dodaných technologií.....	17
8. Požadavky na technický popis řešení v nabídce .....	18

## 1. Zkratky a pojmy

- (1) Zkratky a pojmy užívané v ZD jsou uvedeny v Příloze 3.a. ZD, specifické zkratky a pojmy poplatné zejména této části VZ jsou v následující tabulce.
- (2) Jedná se o podpůrnou informaci, kterou Zadavatel poskytuje pro zachování jednoznačného výkladu textu dokumentu.

Zkratka	Význam
NGFW	Next-Generation Firewall
IPS	Intrusion Prevention System
CPU	Central Processing Unit
RAM	Random Access Memory
RAID	Redundant Array of Inexpensive Disks
HW	Hardware
SW	Software
VLAN	Virtual Local Area Network
LACP	Link Aggregation Control Protocol
LDAP	Lightweight Directory Access Protocol
AD	Active Directory
SNMP	Simple network management protocol
FTP	File Transfer Protocol
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
DDoS	Distributed Denial of Service
VPN	Virtual private network
SSL	Secure Sockets Layer
SSH	Secure Shell
TCP	Transmission Control Protocol
SIEM	Security Information and Event Management
SOAR	Security orchestration, automation and response
NFS	Network File System
VM	Virtual Machine
VDI	Virtual Desktop Infrastructure
IPv4/v6	Internet Protocol version 4 / version 6
RIP	Routing Information Protocol
OSPF	Open Shortest Path First
BGP	Border Gateway Protocol

## 2. Místo plnění

Oblastní nemocnice Kladno, a.s., nemocnice Středočeského kraje, Vančurova 1548, 272 01 Kladno.

## 3. Doba plnění

- (1) Dodávka bude zahájena po nabytí účinnosti smlouvy a bude řízena milníky uvedenými v tabulce Milníky
- (2) Milníky Fáze A instalace a implementace dle Smlouvy.

<b>Id</b>	<b>Činnosti</b>	<b>Termín</b>
<b>01</b>	Podpis Smlouvy	Zadavatel předpokládá 02. 01. 2024
<b>02</b>	Zahájení realizace projektu	do 1. 04. 2024 (navazuje na Část 1 - Zabezpečovací technologie pro 2 serverovny)
<b>Instalace a implementace SYSTÉMU</b>		
<b>03</b>	<b>Zpracování a akceptace Detailního realizačního konceptu</b> Výstupem bude dokument Detailní realizační koncept Předání dílčího plnění a Akceptace dílčího plnění	do 1 měsíce od zahájení realizace projektu
<b>04</b>	<b>Dodávka a instalace technologií</b>	do 2 měsíců od zahájení realizace projektu
<b>05</b>	<b>Zkušební a testovací provoz, migrace stávajících dat objednatele</b> Akceptace Testovacího provozu	do 3 měsíců od zahájení realizace projektu
<b>06</b>	<b>Produkční provoz</b> Akceptace produkčního provozu, akceptace Fáze A Dodávka licencí Ukončení Fáze A,	do 4 měsíců od zahájení realizace projektu

- (3) Fáze B – HW a SW maintenance výrobce technologií a systémů dle Smlouvy bude zahájena ukončením Fáze A (ukončení projektu akceptací produktivního provozu).
- (4) Termín ukončení se může změnit z objektivních příčin, způsobených třetími stranami nebo jinými okolnostmi, nezávislymi na vůli smluvních stran.

#### 4. Způsob prokázání splnění požadavků minimálního plnění

---

- (1) Zadavatel požaduje, aby Dodavatelem nabízená dodávka splňovala veškeré dále uvedené požadavky (funkcionality a parametry) a tyto byly zahrnuty v nabídce Dodavatele a v celkové nabídkové ceně.
- (2) Dodavatel ve své nabídce jednoznačně deklaruje splnění, popřípadě absenci každého níže uvedených požadavků v tabulkách označených jako „Minimální požadavky ...“, a to vyplněním příslušného pole „Splněno“ jedno ze dvou nabízených možností:

„ANO“ v případě že dodávka Dodavatele (Nabídka) minimální požadavek **splňuje**

nebo „NE“ v případě že dodávka Dodavatele (Nabídka) minimální požadavek **nesplňuje**

Zadavatel požaduje po Dodavatelích, aby uvedli informaci o skutečné funkcionalitě nabízeného systému, kterou bude možné ověřit v testovacím provozu, např. v rámci školení administrátorů.

- (3) Nesplnění kteréhokoli ze stanovených minimálních požadavků bude znamenat vyloučení účastníka ze zadávacího řízení.
- (4) Tato kapitola 4 platí pro následující kapitoly 5 až 7.

#### 5. Požadavky na jednotlivé položky přístupové infrastruktury a zálohování

---

- (1) Předmětem této části VZ je dodávka a instalace HW, SW a souvisejících služeb dále specifikovaných v kapitolách 5.1 až 5.3.

##### 5.1. Technická specifikace řízení provozu mezi segmenty sítě (NGFW) vč. detekce bezpečnostních událostí (IPS)

- (1) Po realizaci opatření bude v organizaci funkční systém řízení provozu mezi segmenty, který bude realizovat dvojicí firewallů s vysokou dostupností, zapojených do clusteru zajišťující:
  - segmentaci LAN a výchozí bránu pro komunikaci;
  - oddělení LAN zadavatele od veřejné sítě Internet;
  - VPN koncentrátor, umožňující jak vzdálené připojení klientů, tak případně Site2Site konektivitu proti externím partnerům a organizacím.
- (2) Součástí řešení je požadován i nezávislý centrální management server pro tvorbu a správu bezpečnostních politik, sběr a interpretaci logů a událostí ze síťových prvků nebo auditní log firewall infrastruktury, umožní korelaci a analýzu bezpečnostních incidentů. Nedílnou součástí jsou pak i 3x DAC 3 m pro každý ze dvou firewallů.
- (3) Minimální požadavky na technickou specifikaci řízení provozu mezi segmenty sítě vč. detekce bezpečnostních událostí jsou uvedeny v následující tabulce.

ID	Požadované parametry	Splněno
	<b>Fyzické vlastnosti pro každý node NGFW clusteru</b>	
01	Montáž do standardního 19“ racku pomocí ližin	ANO
02	Formát zařízení max 2U	ANO

03	Napájení z 2 nezávislých zdrojů AC 230V s podporou hotswap	ANO
04	Minimálně 8 fyzických CPU jader, , kde součin počtu jader [ks] a frekvence [Ghz] je nejméně 28	ANO
05	Minimálně 96GB RAM	ANO
06	Minimálně 2x SSD o kapacitě min 400GB RAID1	ANO
07	Minimálně 4x 10GbE SFP+ - dva nezávislé chipset	ANO
08	Minimálně 4x 1/10GbE	ANO
09	1x dedikovaný port pro nezávislý management (rozhraní RS-232 nebo RJ-45)	ANO
<b>Vlastnosti NGFW řešení</b>		
10	Podpora HW akcelerace IP provozu	ANO
11	Podpora IPv4 a IPv6	ANO
12	Podpora HA konfigurace složené alespoň ze dvou prvků	ANO
13	Podpora HA konfigurace v módech active/passive a active/active	ANO
14	Podpora L2 a L3 HA konfigurace	ANO
15	Podpora ISP redundance – připojení min 2 nezávislých Internetových linek a jejich automatické využití	ANO
16	Možnost vytváření zcela oddělených virtuálních instancí	ANO
17	Podpora 802.1Q VLAN – minimálně 1024 VLAN	ANO
18	Podpora VXLAN	ANO
19	Podpora dynamického směrování RIPv2, OSPFv2, OSPFv3, BGP	ANO
20	Podpora 802.3ad LACP	ANO
21	Podpora DNS	ANO
22	Podpora DHCP (klient i server)	ANO
23	Podpora NAT46, NAT64, NAT66	ANO
24	Možnost integrace s 802.1X řešením	ANO
25	Podpora AD, LDAP, RADIUS integrace	ANO
26	Podpora SNMPv2c, v3	ANO
27	Minimální propustnost firewall SPI 20Gbps	ANO
28	Minimální propustnost firewall + IPS + antivirus + URL filtering + Aplikační kontrola + Antibot + NAT + QoS + VPN 5Gbps	ANO
29	Minimální počet konkurenčních spojení 3 000 000	ANO
30	Minimální počet nových spojení 150 000/s	ANO
31	Požadované funkcionality: Firewall, IPS, Aplikační kontrola, Ochrana před Malware, Botnet a Zero-day ochrana, HTTPS kontrola, Sandboxing	ANO
32	Všechny bezpečnostní funkcionality organizovatelné do bezpečnostních politik	ANO
33	Systém nabízí předdefinované IPS politiky	ANO

34	Plná integrace IPS s modulem firewallu	ANO
35	Možnost definice IPS pravidel a výjimek dle kombinace src IP + dst IP + protokol + signatura	ANO
36	Všechny funkcionality NGFW řešení musí provádět úplnou kontrolu každého paketu	ANO
37	Systém musí obsahovat alespoň 5000 předdefinovaných služeb a protokolů	ANO
38	Systém umožňuje SSL/TLS inspekci, podpora TLS1.2, TLS1.3	ANO
39	Systém umožňuje filtrování komunikace už na úrovni DNS	ANO
40	Možnost vytvoření vlastních IOC indikátorů (IP, MD5, URL), manuálně nebo přes API	ANO
41	Funkce sandbox pro emulaci souborů v protokolech SMTP, FTP, SMB a HTTP/S	ANO
42	Systém podporuje technologii Content disarm and reconstruction (CDR) – proaktivní extrakce potencionálně škodlivého obsahu, min podpora grafických souborů, MS Office a pdf	ANO
43	Systém musí být schopný identifikovat útok typu DDoS a Bruteforce	ANO
44	Systém umožňuje získávat identity uživatelů a stanic z AD bez nutnosti instalace software na AD server	ANO
45	Systém umožňuje sdílení identit mezi jednotlivými firewallly bez nutnosti dalších komponent	ANO
46	Integrace s AD na úrovni FW pravidel (user based firewall)	ANO
47	Podpora SSL VPN v režimu tunel a v režimu portal	ANO
48	Podpora IP komprese pro S2S VPN	ANO
49	Podpora algoritmu pro S2S šifrování min AES-256 a integritu SHA-256	ANO
50	SSL VPN terminace pro min 700 souběžných spojení, je-li omezeno licencí, licence pro požadovaný počet musí být součástí nabídky	ANO
51	Podpora multi-faktorové autentizace pro SSL VPN (integrace s Microsoft Authenticator, Email, SMS)	ANO
52	Podpora automatizace pomocí REST API	ANO
53	Management a konfigurace přes SSH	ANO
	<b>Vlastnosti centrálního management a logovacího systému</b>	
54	Management fyzicky oddělený od firewall platformy – možná implementace jako samostatný HW nebo jako SW na virtuálním serveru	ANO
55	Podpora virtualizace VMware	ANO
56	Centrální správa bezpečnostních pravidel a nastavení	ANO
57	Centrální ukládání logů z firewallů na fyzicky oddělený management	ANO
58	Možnost provozování managementu v režimu vysoké dostupnosti	ANO
59	Komunikace mezi management platformou a firewallly musí být autentizovaná a šifrovaná	ANO
60	Možnost prohledávání všech typů logů (FW, IPS, malware) v jednom okně s definováním vlastních filtrů	ANO

61	Možnost export filtrovaných logů do souboru	ANO
62	Možnost konfigurace a ladění IPS modulu přímo z logů	ANO
63	Indexování logů s možností rychlého prohledávání	ANO
64	Funkce centrálního logování s dostupností logů a událostí minimálně 60 dnů zpět	ANO
65	Retence logů minimálně 12 měsíců	ANO
66	Možnost logování a vyhledávání TCP stavových informací jednotlivých spojení (SYN, SYN.ACK, Established, FIN, FIN.ACK, RST)	ANO
67	Možnost přidání popisu pro každé FW pravidlo	ANO
68	Každé pravidlo musí nabízet statistiku počtu užití (hit count)	ANO
69	Možnost časového omezení jednotlivých pravidel	ANO
70	Možnost seskupování firewall pravidel do samostatných logických skupin a oddílů	ANO
71	Systém umožňuje kontrolu chyb a duplicit při vytváření pravidel	ANO
72	Možnost auditu historie změn přímo u vybraného pravidla (změny, čas, kdo...)	ANO
73	Možnost vyhledávání firewall pravidla dle kombinace definovaných atributů (minimálně zdrojová IP, cílová IP, uživatel, služba, aplikace...)	ANO
74	Možnost vyhledat využití objektů (výskyt v aktivních i neaktivních pravidlech, nebo v jiných objektech, např. ve skupinách)	ANO
75	Sytém umožňuje práci a změny v konfiguraci více administrátorů současně, ochrana proti kolizi při současných změnách více administrátory	ANO
76	Možnost definovat přístupových práv administrátorským účtům jen pro určitá firewall pravidla	ANO
77	Možnost definovat oprávnění pro administrátorské účty a profily (read only, zápis, aplikace politik...)	ANO
78	Možnost multi-faktorové autentizace pro přístup k management systému	ANO
79	Konfigurace bezpečnostních politik a nastavení prostřednictvím GUI rozhraní, připojení k GUI šifrovaným kanálem	ANO
80	Podpora automatizace pomocí REST API	ANO
81	Funkcionalita korelace logů, analýzy a správy bezpečnostních událostí s předefinovanými pohledy/dotazy a reporty	ANO
82	Minimálně 1000 korelovaných log záznamů/s (EPS), je-li omezeno licencí, licence pro požadovaný počet korelovaných log záznamů musí být součástí nabídky	ANO
83	Možnost vytváření uživatelsky definovatelných reportů (na základě log záznamů a bezpečnostních událostí), možnost periodických reportů	ANO
84	Možnost integrace se SIEM, SOAR – qRadar, ArcSight, Splunk, LogRhythm	ANO
	<b>Implementace a podpora</b>	
85	Přenesení nastavení ze stávajícího prostředí na dodaný systém	ANO
86	Dokumentace, zaškolení administrátorů zadavatele	ANO



<b>87</b>	Záruka na HW, podpora SW, dostupné aktualizace firmware a bezpečnostních signatur v délce minimálně 5 let	ANO
<b>88</b>	Podpora na 5 let s reakcí následující pracovní den, oprava v místě instalace zařízení	ANO

## 5.2. Technická specifikace serverů pro zálohování

- (1) Pro účely zpracování záloh a obnovu je z bezpečnostního důvodu fyzického oddělení požadováno vytvoření zálohování, které bude řízeno pomocí dvou nezávislých backup serverů. Jeden stávající server bude umístěn v záložní serverovně a druhý – dodaný v rámci tohoto zadávacího řízení bude umístěn v primární serverovně. Metadata budou ukládána společně s daty na disková úložiště backup serverů pomocí protokolu S3.
- (2) Zálohy virtuálních serverů budou probíhat pomocí backup proxy na jednotlivých virtualizačních hostech. Separátní prostředí typu nevirtualizované platformy budou zálohována pomocí agentů umístěných přímo v prostředí operačního systému. Zálohování bude probíhat přímo ze zdroje na cíl záloh. Prvotním cílem záloh bude diskové pole pro nestrukturovaná data, kde bude umístěna první instance záloh určená pro rychlou obnovu. Kapacita zálohy bude odpovídat 1:1.5 kapacitě zdrojových dat. Data budou následně připravována pro archivaci na již mnohem pomalejší disky zálohovacího serveru, které slouží převážně pro archivační úlohy.
- (3) Zálohovací servery budou sloužit primárně jako management pro ukládání záloh. Sekundární role bude úložiště pro sekundární data záloh a dále prostředí pro konsolidaci dat před započítáním archivace.
- (4) Minimální požadavky na technickou specifikaci 1 ks zálohovacího serveru jsou uvedeny v následující tabulce.

ID	Požadované parametry	Splněno
<b>01</b>	Montáž do standardního 19" racku o maximální výšce 2 RU, chassis pro min. 24x 3,5" disků + 8x 2,5" disků	ANO
<b>02</b>	Minimálně jeden 24-jádrový procesor s hodnotou dle SPECrate®2017_int_base min. 155 a SPECrate®2017_fp_base min. 160 pro 1 CPU konfiguraci (údaje musí být k dispozici na <a href="http://www.spec.org">www.spec.org</a> )	ANO
<b>03</b>	Min. 256 GB RAM (min. 32GB moduly 3200MT/s s podporou ECC), server s celkem 24 DIMM pozicemi, každý paměťový kanál musí být osazen nejméně jedním modulem, všechny paměťové moduly musí být identické. Podpora rozšiřitelnosti až na min. 1,5TB RAM per server.	ANO
<b>04</b>	Min. 8x 960GB 2,5" SATA SSD pro operační systémy	ANO
<b>05</b>	Min. 2x diskový SAS/SATA kontrolér o celkové cache minimálně 8GB a podporou RAID	ANO
<b>06</b>	Min. 24x 10TB 3,5" SATA HDD (7.2k RPM) pro data záloh	ANO
<b>07</b>	Min. 4x 10/25GbE SFP28 porty na dvou nezávislých síťových kartách	ANO
<b>08</b>	Management serveru nezávislý na operačním systému s možností zapnutí, vypnutí, restartu serveru, přesměrování KVM nezávisle na OS, vzdálené připojení médií, časově neomezená licence	ANO
<b>09</b>	Management musí podporovat dvoufaktorovou autentizaci, filtrování přístupu na základě IP adres (IP blocking) a AD/LDAP, podpora Silicon Root Of Trust, Secure Boot a TPM 2.0	ANO
<b>10</b>	Pro management požadujeme vestavěné GUI s podporou HTML5 a možnost komunikace pomocí: HTTPS, CLI, IPMI, REDFISH	ANO
<b>11</b>	Nejméně 2 redundantní, za chodu vyměnitelné napájecí zdroje s platinovou účinností min. 1500W každý	ANO
<b>12</b>	Rackové ližiny a rameno na kabeláž na zadní straně serveru	ANO

13	Dodání včetně 4x SFP28 twinaxial kabelů o délce 3m pro každý server	ANO
14	Certifikace pro VMware 6.7u3 a vyšší, Windows Server 2016 a vyšší, Red Hat Enterprise Linux a SUSE Linux Enterprise Server	ANO
15	Schopnost napojení na dohledové centrum výrobce s funkcí automaticky generovat servisní události	ANO
16	Licence na Microsoft Windows Standard 2019 na všechna CPU jádra	ANO
17	Podpora na 5 let s reakcí následující pracovní den, oprava v místě instalace zařízení.	ANO

- (1) Součástí řešení pro ochranu před kybernetickými hrozbami (kryptoviry) nebo chybou uživatele je i zálohovací software. Kontrola funkčnosti záloh bude probíhat automatizovaně a plánovaně.
- (2) Minimální požadavky na technickou specifikaci software pro zálohování jsou uvedeny v následující tabulce.

ID	Požadované parametry	Splněno
01	Zálohovací software (SW) s prokázanou kompatibilitou s VMware prostředím verzí 6.5/6.7/7.0/8.0.	ANO
02	Zálohovací SW musí poskytovat podporu hostitelů spravovaných serverů VMware vCenter Server a samostatné hostitele bez nutnosti instalace agentské aplikace pro zálohování/obnovu virtuálních počítačů.	ANO
03	Licencování zálohovacího SW podle počtu zálohovaných instancí pro využití s různými typy workloadů, včetně on-premise, cloudových, fyzických serverů a enterprise aplikací. Licencovaný SW musí pracovat na jakémkoliv HW (serveru, úložišti). Nesmí být nabídnut SW licencovaný podle back end ani front end kapacity zálohovaných aktiv.	ANO
04	Zálohovací SW poskytuje zálohu sdílených souborů ze zařízení NAS zařízení pomocí (protokolem SMB a NFS) a přímo ze souborových systémů serverů s OS Windows a Linux.	ANO
05	Výstupem zálohovacího SW musí být samostatné souborové backup archivy pro snadnou přenositelnost záloh. Archivy je možné vytvářet na základě zálohovací úlohy nebo na úrovni virtuálního serveru.	ANO
06	Zálohovací SW podporuje běžné režimy zálohování – úplná záloha (full), syntetická úplná, přírůstková záloha (incremental) a zpětný přírůstkový režim.	ANO
07	Zálohovací SW podporuje kompresi a deduplikaci dat zálohy. Využití deduplikace a komprese nesmí omezovat funkce zálohovacího SW deklarované v jeho technické specifikaci.	ANO
08	Zálohovací SW umožňuje integraci s enterprise primárními blokovými úložišti předních výrobců diskových polí s podporou orchestrace pro zajištění generování aplikačně konzistentních snapshotů (včetně logických disků replikovaných na úrovni diskového pole). SW musí zajistit integraci s nabízeným typem diskových polí pro strukturovaná data.	ANO
09	Dedupliční metadata musí být uložena přímo v souborech záloh. Pro dedupliční metadata nesmí zálohovací SW využívat centrální dedupliční databázi. Použitelnost záložních souborů nesmí být ovlivněna nefunkčností databáze zálohovacího SW.	ANO

ID	Požadované parametry	Splněno
10	Zálohovací SW musí disponovat uživatelskou samoobslužnou aplikací (portálem), která bude umožňovat uživatelům služby obnovy záloh – pro soubory, virtuální počítače, objekty MS Exchange a databáze MS SQL a Oracle (včetně obnovení v čase).	ANO
11	Zálohovací SW musí poskytovat dokumentovaný REST API interface pro integraci s dalšími systémy, zejména s nabízeným úložištěm pro nestrukturovaná data.	ANO
12	Zálohovací SW musí mít implementovanou podporu šifrování celého síťového provozu mezi všemi komponentami SW a také šifrování souborů záloh na cílovém úložišti. Šifrování nesmí omezovat žádné funkcionality popsané v technické specifikaci.	ANO
13	Zálohovací SW musí podporovat mechanismus pro sledování blokových změn CBT (Change Block Tracking). Implementace CBT musí být certifikována výrobcem hypervizoru pro všechny podporované hypervizory.	ANO
14	Zálohovací SW podporuje kopírování bodů obnovy a replikaci virtuálních serverů do vzdáleného umístění a také funkcionality WAN akcelerace.	ANO
15	Zálohovací SW musí podporovat replikaci produkčních VM přímo z infrastruktury VMware vSphere mezi hostiteli ESXi, včetně asynchronní nepřetržité replikace (CDP). Umožňuje také využívání souborů se zálohami jako zdroje pro replikační úlohy.	ANO
16	Zálohovací SW umožňuje okamžitou obnovu i více VM současně přímo ze souborů se zálohou, a to z libovolného bodu obnovy, s podporou této funkce ve VMware prostředí. Funkce musí být nezávislá na použitém hardwaru pro ukládání záložních souborů VM. SW musí poskytovat okamžitou obnovu souborových dat ze zálohy úložišť NAS pomocí protokolu CIFS/SMB.	ANO
17	Zálohovací SW podporuje vytváření virtuálních laboratoří/izolovaných prostředí pro infrastrukturu VMware pomocí spuštění VM strojů přímo ze souborů záloh. Pro VMware funguje vytváření tohoto prostředí přímo ze snímků úložiště vytvořených na podporovaných zařízeních.	ANO
18	Zálohovací SW má implementované mechanismy ověřování obnovy dat ze zálohy, které zajistí testování obnovy VM v izolovaném síťovém prostředí na infrastruktuře VMware. Ověřovací mechanismy musí umožňovat plánovatelné a automatizované testování aplikací uvnitř VM pomocí vlastních nebo předdefinovaných skriptů.	ANO
19	Navrhované řešení musí zajistit licencování zálohování minimálně pro 50 virtuálních serverů.	ANO
20	Podpora na 5 let s reakcí následující pracovní den	ANO

### 5.3. Technická specifikace serverů a diskových polí

- (1) Pro zajištění vysoké dostupnosti výpočetních clusterů bude zbudována nová záložní výpočetní farma. Farma bude navržena na virtualizovaném serverovém clusteru (virtualizační technologie VMware vSphere). Výpočetní farmy budou doplněna o all-flash disková pole. Nová výpočetní farma bude v režimu vysoké dostupnosti ke stávajícím technologiím, které jsou taktéž postaveny na technologii VMware vSphere a aktuálně neřeší redundanci ani v rámci jednoho datového centra (žádný sdílený úložný prostor pro strukturovaná data).
- (2) Budou dodána dvě disková pole pro strukturovaná a dvě pro nestrukturovaná data.

(3) Disková pole pro strukturovaná data budou plnit potřebu uniformního vMSC clusteru pro technologii VMware.

### 5.3.1 Disková pole pro strukturovaná data

(4) Diskové úložiště je určeno k ukládání strukturovaných (blokových) dat virtualizované výpočetní farmy, případně dat fyzických serverů

(5) Minimální požadavky na technickou specifikaci dodání 1 ks diskového pole pro strukturovaná data jsou uvedeny v následující tabulce.

ID	Požadované parametry	Splněno
01	Montáž do standardního 19" racku o maximální výšce 4 RU	ANO
02	Diskové pole musí být typu All Flash – NVMe pole s disky podporujícími PCI Gen4 technologii	ANO
03	Podpora aktuální verze nepoužívanějších OS min. VMware vSphere 8.0, Windows 2022, RedHat Linux 9, Ubuntu 22.04	ANO
04	Diskové pole musí poskytovat min.hrubou (RAW) kapacitu 20TB. Tato kapacita bude očištěna o systémovou a spare kapacitu a s využitím technik datové redukce bude dostupná kapacita pro ukládání dat alespoň 25TB	ANO
05	Diskové pole musí být flexibilně škálovatelné tj. podporovat škálování scale-up přidáváním NVMe diskových polic i scale-out pomocí zabudovaného klastrování	ANO
06	Diskové pole musí být škálovatelné alespoň na 24 NVMe disků v rámci řadiče a musí být v budoucnu rozšiřitelné min. na dvojnásobek disků v přídatných NVMe diskových policích	ANO
07	V případě scale-out rozšiřování musí být možné rozprostřít LUNy přes všechny řadiče škálovatelného úložiště	ANO
08	Diskové pole musí být dodáváno s nejméně 64GB cache na jeden řadič pro operace čtení a zápisu	ANO
09	Operace zápisu musí být zcela chráněny a v případě výpadku napájení nesmí dojít ke ztrátě dat. Tento mechanismus se nesmí spoléhat na baterie	ANO
10	Diskové pole nesmí obsahovat Single Point Of Failure tj. musí být odolné min. proti výpadku jedné komponenty typu řadiče, zdroje, cache, ventilátoru, HBA apod	ANO
11	Výpadek žádné komponenty včetně řadiče diskového pole nesmí způsobit pokles požadovaného výkonu diskového pole	ANO
12	Během kritických podpůrných činností, jako je aktualizace Firmware, aplikaci patche atd., musí být pole dostupné a nesmí dojít k degradaci výkonu	ANO
13	Diskové pole poskytuje na front-end portech diskového pole min. takovýto ustálený výkon: 55 tis.IOPS pro 100% random zátěž, velikost bloku 8kB a poměr čtení zápis 50/50; 2GB/s sekvenční čtení a 700MB/s sekvenční zápis při velikosti bloku 256kB	ANO
14	Diskové pole musí být odolné proti výpadku až tří disků současně. V případě, že to výrobce nepodporuje, pak RAID pole musí mít velikost maximálně 6D+2P	ANO
15	Diskové pole musí být možné povýšit na novější generaci výměnou řadičů, aniž by bylo nutné měnit disky a případné diskové police	ANO
16	Povýšení na novější generaci musí být možné provést bez odstávky diskového pole	ANO
17	Diskové pole musí být dodáno min. s dvěma řadiči a 4x 25Gb IP porty. (každý front-end PCI slot musí mít nejméně 8 linek PCI Gen4)	ANO
18	Diskové pole musí mít také podporu pro 100Gb ETH porty (pro případné rozšíření)	ANO
19	Diskové pole musí podporovat nastavení Quality of Services (QoS) na úrovni LUN nebo VMware vVol s granularitou nastavení min. na úrovni IOPS a MB/sec	ANO

ID	Požadované parametry	Splněno
20	Diskové pole musí podporovat tyto funkce - inline de-duplikace, komprese a thin provisioning	ANO
21	Diskové pole musí podporovat ne-deduplikované a duplikované LUNy současně	ANO
22	Diskové pole musí podporovat synchronní i asynchronní replikaci dat mezi diskovými poli	ANO
23	Disková pole musí umět vytvořit jedno logické pole pro vytvoření storage geo-klastru s automatickým transparentním failoverem mezi lokalitami a funkcionalitou svědka na třetí lokalitě pro zabránění split-brain syndromu	ANO
24	Diskové pole musí mít schopnost replikovat data z All Flash do Hybridního diskového pole, nebo naopak v rámci dané rodiny polí	ANO
25	Prodejce poskytne licence pro všechny požadované funkce, jako je Snapshot, Clone, Replikace, QoS, management apod., pro celkovou kapacitu pole; Pro budoucí zvýšení kapacity nebude vyžadována žádná dodatečná softwarová licence; Jakákoli dodatečná licence vyžadovaná pro splnění technické specifikace musí být nabídnuta předem	ANO
26	Podpora na 5 let s reakcí následující pracovní den, oprava v místě instalace zařízení	ANO

### 5.3.2 Disková pole pro nestruturovaná data

(6) Pro nestruturovaná data bude k dispozici úložiště postavené na technologii scale-out. Cílem fungování tohoto úložiště je zajištění bezpečného místa pro uložení objemných souborů jako jsou například PACS data a data záloh.

(7) Minimální požadavky na technickou specifikaci 1 ks diskového pole pro nestruturovaná data jsou uvedeny v následující tabulce.

ID	Požadované parametry	Splněno
01	Montáž - maximální výšce 8 RU standardního racku 19"	ANO
02	Scale out architektura – minimálně 4 identické redundantní nod s technologií erasure coding (EC). Vyžaduje se odolnost úložiště vůči výpadku alespoň jednoho HW nodu a nejméně dvou disků z každého jednoho nodu	ANO
03	V produkčním nasazení bude pole využívat protokol NFS (v4.1) a protokol SMB (v3)	ANO
04	Diskové pole bude podporovat protokol S3 pro přesouvání záloh. Musí mít vlastní dokumentované REST API pro úplnou správu pole a diskového prostoru přímo z aplikace	ANO
05	Diskové pole poskytuje funkce pro replikaci mezi dvěma diskovými poli na úrovni souborové vrstvy s kontinuálním průběhem (připouští se synchronní i asynchronní replikace)	ANO
06	Diskové pole pro získání identit/stromu přístupových oprávnění umí přistupovat do uživatelského stromu Microsoft Active Directory a Linux LDAP (obě funkce, nikoliv však souběžně)	ANO
07	Řešení musí evidovat přístupové seznamy, zejména pro protokol NFS; Bezpečnost musí být vázána k souboru a k uživatelské identitě přistupujícího uživatele. Minimální požadavky na rozpoznání příznaků jsou pro čtení, zápis a řízení oprávnění k souboru;	ANO
08	Pro uživatele musí být diskové pole prezentováno jako jeden name space. Požaduje se integrovaný load balancer pro rovnoměrné rozložení zátěže mezi uzly	ANO
09	Řešení musí podporovat vytváření snapshotů s vytvářením zámků na dané souborové struktuře pro zabránění manipulace se soubory; V kombinaci se zálohovacím SW musí tato funkce zajistit repositář záloh se zárukou nezměnitelnosti souborů	ANO

ID	Požadované parametry	Splněno
10	Diskové pole musí podporovat šifrování dat (data at rest encryption), minimálně na úrovni AES-256. Šifrování nesmí být závislé na hardware pro zajištění bezpečné přenositelnosti dat mezi různými hardwarovými platformami; Řešení musí zajistit bezpečnou ochranu média proti krádeži dat i po vyřazení médií z produkčního provozu, musí obsahovat interní transparentní správu klíčů a spolehlivý mechanismus pro efektivní rotaci šifrovacích klíčů	ANO
11	Data uložená na diskovém poli budou komprimována a potenciálně i šifrována. Funkce deduplikace a komprese není požadována; Deduplikační a kompresní poměr nelze započíst do stanovení celkové kapacity pole. Požadovaná čistá kapacita pole je nejméně 75 TB	ANO
12	Požadovanou kapacitu diskového úložiště bude možné využít celou; Jestliže například výrobce doporučuje využívat pole do 90 % jeho dodané kapacity, zadavatel vyžaduje navýšit dodanou kapacitu podle doporučení výrobce	ANO
13	Diskové pole bude běžně sloužit pro paralelní přístup systému i uživatelů. Pole musí být schopno spolehlivě obsloužit současnou komunikaci s nejméně 1000 uživateli a 100 systémy (NFSv4.1); Jedna instance diskového pole musí mít nejméně 48 CPU jader s minimální základní frekvencí nejméně 2 GHz	ANO
14	Diskové pole poskytuje minimálně čtyři 25GbE front end porty a čtyři 25GbE back end porty, které je v případě sdílení možné libovolně kombinovat. Celkový nejmenší počet portů je osm; Každý uzel musí disponovat minimálně dvěma porty	ANO
15	Výkon diskového pole musí být minimálně 40 000 IOPS (NFSv4.1); Celkový výkon pole pro čtení musí být větší než 4 GB za vteřinu a celkový výkon pro zápis nejméně 2 GB za vteřinu. Jedno spojení musí zapisovat rychlostí minimálně 1 GB za vteřinu a číst rychlostí 1,5 GB za vteřinu. Výkon musí být pole schopné využít 100% požadované kapacity	ANO
16	Pro zajištění požadavku navýšení diskové kapacity musí být pole rozšiřitelné minimálně na pětinasobek úvodní kapacity (375TiB); Rozšíření kapacity musí být provedeno formou scale-out přidáváním identických nodů; Zadavatel reálně plánuje rozšíření na více než dvojnásobek úvodní kapacity; Požadavky na rozšířené pole jsou následující: 300 000 IOPS (NFSv4.1), celkový výkon pro čtení 20 GB za vteřinu a výkon pro zápis nejméně 10 GB za vteřinu; Pole po rozšíření musí splňovat požadavek na možnost dalšího rozšíření o minimálně další dvojnásobek své diskové kapacity	ANO
17	Podpora na 5 let s reakcí následující pracovní den, oprava v místě instalace zařízení	ANO

## 6. Fáze A - Instalace a implementace

- (1) Instalace a implementace technologií popsaných v kapitolách 5.1 až 5.3 bude provedena v jednotlivých požadovaných krocích a termínech uvedených v kapitole 3.
- (2) Minimální požadavky na Instalaci a implementaci technologií jsou uvedeny v následující tabulce.

Id	Plnění požadavku	Splněno
1	Kompletní instalace, konfigurace a montáž dodaného HW a SW v prostorách zadavatele	ANO
2	Instalace a konfigurace SW	ANO
3	Instalace a konfigurace všech požadovaných funkcionalit	ANO

<b>Id</b>	<b>Plnění požadavku</b>	<b>Splněno</b>
<b>4</b>	Testování funkčnosti (provedení testů všech technologií a systémů)	ANO
<b>5</b>	Základní uživatelské seznámení a proškolení administrátorů s dodanými technologiemi	ANO
<b>6</b>	Vypracování dokumentace realizovaného řešení zahrnující instalační protokoly a instalační postupy.	ANO

## **6.1. Zpracování a akceptace Detailního realizačního konceptu**

- (1) Dokument Detailní realizační koncept bude obsahovat minimálně:
  - a) definici cílového stavu, která bude vycházet z požadavků na budoucí stav, viz tento dokument,
  - b) akceptační kritéria cílového stavu;  
pro ověření plnění Dodavatele v rámci Smlouvy jsou uvedena v tomto dokumentu, a to v tabulkách označených „Minimální požadavky ...“, kde Dodavatel bude deklarovat svoji připravenost poskytovat bezvadné plnění již v rámci Zkušebního (testovacího) provozu.
  - c) detailní harmonogram realizace zakázky, který vychází z milníků uvedených v kapitole 3 a z Dodavatelem navrženého Harmonogramu projektu.
- (2) Formálně bude tato oblast Fáze A završena dohodnutým a vzájemně odsouhlaseným Předávacím protokolem dílčího plnění (Dodavatel předává dokument Detailní realizační projekt) a Akceptačním protokolem dílčího plnění, kterým Zadavatel akceptuje splnění podmínek této části Fáze A ve Smlouvě.

## **6.2. Předání a převzetí plnění**

### **6.2.1. Předání a převzetí dokumentů**

- (1) Dokumenty, které mají být vypracovány Dodavatelem a které se poskytují Zadavateli jako součást poskytování díla (zejména Detailní realizační koncept), budou nejdříve předloženy Zadavateli ve formě návrhu k posouzení.
- (2) Dodavatel se zavazuje předat první verzi dokumentu Zadavateli k akceptaci ve lhůtě domluvené mezi Dodavatelem a Zadavatelem na základě Smlouvy, nebo jinak stanovené v souladu se Smlouvou.
- (3) Zadavatel je oprávněn ve lhůtě pěti (5) pracovních dnů od doručení příslušného dokumentu písemně předložit Dodavateli své připomínky k návrhu.
  - a) Po diskusi o těchto připomínkách upraví Dodavatel příslušný návrh v souladu s dohodnutými změnami a se zpracováním těchto dohodnutých změn jej předá ve stejné lhůtě pěti (5) pracovních dnů Zadavateli.
  - b) V případě, že Zadavatel nemá k předaným dokumentům výhrady, považují se za převzaté k okamžiku doručení jejich konečné verze Zadavateli.
  - c) V případě, že Zadavatel připomínky ve lhůtě pěti (5) dnů nepředloží, má se za to, že s předloženým dokumentem souhlasí a dokument se považuje za řádně převzatý.

### **6.2.2. Předání a převzetí ostatních plnění dle Smlouvy (vyjma služeb)**

- (1) V případě, že součástí poskytování plnění Dodavatelem dle Smlouvy je plnění, které podléhá akceptaci Zadavatelem, musí dojít k podpisu Předávacích protokolů ohledně tohoto plnění v termínech uvedených v harmonogramu, není-li výslovně uvedeno jinak.

Detailní kritéria akceptace a vymezení plnění, která podléhají akceptaci Zadavatelem, jsou uvedena v tomto dokumentu, případně v Detailním realizačním projektu.

Jestliže plnění nebo jeho jednotlivé části splní kritéria akceptačního řízení, považují se za řádně ukončené a Zadavatel je povinen je převzít.

(2) Akceptační procedury zahrnují porovnání skutečných vlastností plnění se závaznou specifikací předmětu plnění dle Smlouvy.

- a) Akceptační procedura bude zahrnovat akceptační testy, které budou probíhat na základě specifikace akceptačních testů obsahující popis testů, testovací data, příslušné prostředí, pořadí provádění testů a akceptační kritéria.

Nedohodnou-li se smluvní strany jinak, vypracuje specifikaci akceptačních testů Dodavatel a předá Zadavateli k odsouhlasení v termínu pěti (5) pracovních dnů před zahájením akceptační procedury dle harmonogramu.

Odsouhlasení bude provedeno písemnou formou v termínu pěti (5) pracovních dnů před zahájením akceptační procedury. Jestliže se Zadavatel v této lhůtě ke specifikaci akceptačních testů písemně nevyjádří, má se za to, že specifikaci akceptačních testů odsouhlasil.

Jestliže Zadavatel specifikaci akceptačních testů v uvedené lhůtě neodsouhlasil, je povinen Zadavatel v této lhůtě sdělit připomínky k Dodavatelem předložené specifikaci akceptačních testů a poskytnout Dodavateli veškerou potřebnou součinnost k dokončení a odsouhlasení specifikace akceptačních testů.

Lhůta pro provedení akceptačních testů a lhůta pro předání plnění nebo jeho části se prodlužuje o dobu, o kterou se prodloužilo písemné odsouhlasení specifikace akceptačních testů z důvodu připomínek na straně Zadavatele oproti lhůtě stanovené.

- b) Dodavatel bude písemně informovat Zadavatele, resp. jeho oprávněné osoby nejméně pět (5) dní předem o termínu zahájení akceptačních testů.

Zadavatel je oprávněn se těchto testů zúčastnit a osvědčit jejich konání, a to formou předávacího protokolu (nebo dílčích předávacích protokolů), podepsaného (podepsaných) oprávněnými osobami obou smluvních stran. Pokud se Zadavatel nedostaví v termínu určeném pro provedení akceptačních testů, ačkoli byl s tímto termínem řádně seznámen, je Dodavatel oprávněn provést příslušné akceptační testy bez jeho přítomnosti.

Takto provedené akceptační testy se považují za provedené v přítomnosti Zadavatele. Kopie veškerých dokumentů vypracovaných v souvislosti s provedením těchto akceptačních testů budou Zadavateli poskytnuty do pěti (5) dnů.

- c) Základním předpokladem pro řádné předání plnění (nebo jeho části) Dodavatelem a převzetí tohoto plnění (nebo jeho části) Zadavatelem, a to formou předávacího protokolu podepsaného oprávněnými osobami obou smluvních stran je skutečnost, že plnění splní kritéria akceptačních testů uvedená v dohodnutých kontrolních specifikacích a bude provedeno v souladu se závaznou specifikací předmětu plnění dle Smlouvy.

- d) Jestliže plnění nebo jeho část splní akceptační kritéria akceptačních testů, Dodavatel se zavazuje v den následující po ukončení akceptačních testů umožnit Zadavateli plnění nebo jeho část převzít a Zadavatel se zavazuje v tomto termínu plnění nebo jeho část převzít.

Pokud Zadavatel plnění nebo jeho část v tomto termínu nepřevzme, ačkoli převzetí plnění nebo jeho části bylo Dodavatelem řádně umožněno, má se za to, že plnění nebo jeho část bylo řádně předáno a Zadavatelem převzato právě v den následující po ukončení akceptačních testů.

- e) Jestliže plnění nespĺňuje stanovená akceptační kritéria kteréhokoliv akceptačního testu, budou výsledky akceptačního testu (splněno/nesplněno/s výhradami) spolu s uvedením termínů pro nápravu uvedeny ve vyhodnocení Akceptačního protokolu.

Dodavatel napraví tyto nedostatky a příslušné akceptační testy budou provedeny znovu.

Tento proces testování a následných oprav se bude opakovat, přičemž výše uvedená ustanovení se použijí obdobně.



Proces testování a následných oprav lze opakovat, dokud Dodavatel nesplní veškerá akceptační kritéria pro příslušný akceptační test, nejvýše však natřikrát (3x).

V situaci, kdy by bylo nutné opakovat akceptační testy více jak třikrát (3x) pro konkrétní fázi projektu, je v takovém případě nutný souhlas nadřízeného orgánu projektu – tzn. řídicího výboru nebo ředitelů projektu dle použité metodiky řízení projektu.

- f) Žádný akceptační test se však nebude považovat za nesplněný, jestliže daný nedostatek nebyl způsoben Dodavatelem, nebo byl zjištěn nebo měl být zjištěn Zadavatelem před nebo při předcházejícím akceptačním testu, ale nebyl v té době oznámen Dodavateli, nebo byl nepodstatný, tzn., neměl vliv na řádné poskytování funkčnosti díla nebo jeho části tak, jak jsou vymezeny ve Smlouvě.
- g) Při převzetí plnění nebo kterékoliv jeho části v souladu s tímto článkem je Zadavatel povinen podepsat potvrzení o přijetí plnění nebo dané části a Zadavatel i Dodavatel se zavazují podepsat příslušný předávací případně akceptační protokol (díličí předávací případně akceptační protokoly), tj. potvrzení o předání a přijetí (převzetí) plnění nebo jeho určité části.

### 6.3. Školení

- (1) Dodavatel poskytne školení pro administrátory IS tak, aby byli schopni řádně užívat, respektive administrovat, instalované technologické části specifikované v kapitole 5.

### 6.4. Dokumentace

- (1) Dodaná dokumentace slouží k zachycení a vyhodnocování plánovaných činností a též k dokumentaci skutečného stavu.

## 7. Fáze B – provozní podpora dodaných technologií

- (1) Požadavky, které musí dodavatel minimálně naplnit na provozní podporu dodaných technologií, jsou v níže uvedené tabulce.

Id	Plnění požadavku	Splněno
01	V rámci běžného rozvoje jednotlivých částí serverové, datové a komunikační infrastruktury Dodavatel zajistí poskytnutí aktualizovaných verzí SW nejpozději do 1 měsíce po uvolnění nové verze k distribuci.	ANO
02	Budou poskytovány informace o změnách a nových funkcích v aktualizovaných verzích instalované technologie.	ANO
03	Bude prováděna průběžná aktualizace dokumentace k programovému vybavení tak, aby u Zadavatele byla vždy aktuální dokumentace k provozované technologii.	ANO
04	Bude poskytována součinnost při zásadním upgrade softwarových částí instalované infrastruktury na vyšší verze.	ANO
05	Bude zajištěna udržitelnost SW třetích stran, dodaných Dodavatelem v rámci veřejné zakázky.	ANO
06	HW a SW maintenance výrobce budou poskytovány po celou dobu smluvního vztahu (min 60 měsíců ode dne protokolárního ukončení Fáze A dle Smlouvy).	ANO
07	Technická podpora a servis zařízení HW a SW budou zabezpečeny Dodavatelem, případně prostřednictvím odpovídajícího servisního kanálu výrobce.	ANO
08	Technická podpora a servis budou realizovány v místě Zadavatele.	ANO

Id	Plnění požadavku	Splněno
	Výjimku tvoří činnosti realizované vzdáleným připojením Dodavatele, výrobce zařízení do prostředí Zadavatele.	
09	Veškeré požadavky budou evidovány v systému servisní podpory Dodavatele nebo výrobce zařízení (HelpDesk).	ANO
10	Kontaktní místo umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím služby HelpDesk, popř. služby Hot-line.	ANO
11	Služba Hot-Line umožní příjem požadavku na servisní zásah v českém jazyce na telefonním čísle: (uvede dodavatel) v režimu <b>5x8 (8 hodin v pracovní dny) v době od 09:00 do 17:00 hod</b> , příjem požadavku bude zajištěn lidskou obsluhou.	ANO
12	Služba HelpDesk umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím webového rozhraní v režimu 7x24 (nepřetržitě vyjma nahlášených servisních zásahů Dodavatele při správě systému HelpDesk).	ANO
13	Služba HelpDesk umožní Zadavateli upřesnit nebo doplnit požadavek.	ANO
14	Služba HelpDesk bude Zadavateli poskytovat přehled o aktuálně nahlášených požadavcích, jejich stavu a aktuálním způsobu jejich řešení.	ANO
	Služba HelpDesk bude Zadavateli zasílat notifikace o změně stavu jeho požadavku (např. zadaný, v řešení, uzavřený atd.) a musí Zadavateli umožnit schvalování uzavření nahlášeného požadavku.	
15	Služba HelpDesk bude poskytovat Zadavateli přístup i k uzavřeným požadavkům a způsobu jejich řešení, bude poskytovat podrobné údaje o historii požadavků od jejich nahlášení, po jejich vyřešení.	ANO

## 8. Požadavky na technický popis řešení v nabídce

(1) Specifikace předmětu plnění:

a) Přehled plnění požadovaných minimálních parametrů;

Dodavatel vloží vyplněný tento dokument doplněný u jednotlivých položek označených jako „Minimální požadavky ...“.

b) Technický popis řešení - grafické schéma a podrobný popis nabízených technologií a systémů;

(2) Dodavatel uvede detailní popis rozhraní jednotlivých technologií pro napojení jiných (stávajících) IS Zadavatele;

(3) Rozsah školení vč. uvedení počtu dní školení navrženého Dodavatelem;

(4) Návrh Metodiky řízení projektu a Harmonogramu projektu.