Veřejná zakázka	**Zálohovací diskové úložiště**
Zadávací řízení	Uzavřená výzva
Limit veřejné zakázky	Malého rozsahu
Druh zakázky	Dodávky
Předpokládaná hodnota veřejné zakázky	2 900 000,- Kč bez DPH
Zadavatel	Mikrobiologický ústav AV ČR, v. v. i.
Adresa	Vídeňská 1083, 142 20 Praha 4
IČ	61388971
Zastoupený	Ing. Jiří Hašek, CSc., ředitel
Profil zadavatele:	https://www.vhodne-uverejneni.cz/profil/mikrobiologicky-ustav-av-cr-v-v-i

Storage	
Parametr storage	**Specifikace – minimální požadavek zadavatele**
Form Factor a vnitřní uspořádání	Diskové pole o max. velikosti 11U, min. 2 Storage procesory, barevně značené hot-plug vnitřní komponenty
Paměť	• min. 64GB cache paměti na každý Storage Procesor, zálohovaná baterií, která zajistí uložení obsahu cache do persistentní paměti
Diskový subsystém	• Hybridní systém diskového pole • Podpora hot-plug disků • All-flash subsystém složený z min. 5x 400GB SSD RAID5 plus min. jeden spare disk • Minimální hrubá kapacita HDD 416 TB bez deduplikačních a kompresních algoritmů. Ochrana dat alespoň na úrovni RAID 6 nebo ekvivalentní dual parity, s minimálně 36 disky pro dosažení požadovaného výkonu. Minimálně dva spare disky nebo odpovídající vyhrazený spare prostor, který není započítán do minimálních parametrů • Možnost rozšíření až na 490 disků • Možnost rozšířit jak o HDD, tak SSD disky • Maximální RAW kapacita alespoň 2,1 PB • Podpora minimálně pro RAID 1/0, 5, 6 nebo ekvivalentní metody ochrany datových bloků

Požadované Funkce	• Midrange diskové pole s Unified funkcionalitou a architekturou Active-Active, bez nutnosti dodatečných file/block gateway
	• Možnost nastavení retenčních zámků pro soubory v NAS minimálně ve dvou úrovních:
	• Ochrana proti úpravám a mazání souborů prostřednictvím protokolů SMB, NFS a FTP
	• Zamezení jakémukoliv mazání, včetně souborového systému, dokud nevyprší všechny časové zámky
	• Podpora thin-provisioningu
	• Automatizovaná tvorba snapshotů
	• Možnost šifrování všech dat uložených na discích pomocí prostředků diskového pole
	• Podpora replikace blokových dat (synchronní i asynchronní) a NAS (minimálně asynchronní)
	• Virtualizační API minimálně pro VMware VAAI a VASA a Windows Hyper-V (ODX a OffloadCopy for File)
	• Podpora VVols
	• Integrace s Veeam Backup & Replication v12 alespoň pro funkce:
	  ○ Backup from Storage Snapshots
	  ○ Veeam Explorer for Storage Snapshots
	  ○ OnDemand Sandbox for Storage Snapshots
	  ○ Licenční výbava diskového pole musí umožňovat integraci se zálohovacím systémem Veeam Backup & Replication verze 12, který zadavatel provozuje. Integrace musí podporovat správu snapshotů (vytváření, rušení), zálohu a obnovu ze storage snapshotů. Podpora integrace (Storage Snapshot Integration) musí být doložitelná výpisem z Veeam Alliance Partner Integrations & Qualifications (https://www.veeam.com/alliance-partner-integrations-qualifications.html)
	  ○ Všechny potřebné licence musí být součástí dodávky
	• Protocol-Endpoints pro zajištění datové cesty přes oba kontrolery
	• Podpora přístupových protokolů NFS, SMB 3.0 (CIFS), iSCSI a Fiber Channel
	• Maximální rozšiřitelnost Lunů a File systému až na 200 TB
	• Možnost přímého připojení iSCSI i FC k serverům
	• Možnost nastavení limitu I/O operací nebo propustnosti pro blokovou a VVol část kapacity
	• Podpora deduplikace a komprese dat
	• Veškeré licence musí pokrývat celé diskové pole nebo celkovou maximální přípustnou kapacitu

Napájení	• Redundantní síťové napájecí zdroje, včetně 2 m napájecích kabelů k poli
Front-end	• Minimálně čtyři 32Gb FC porty na každý Storage procesor • Minimálně čtyři 25Gb/s SFP porty na každý Storage procesor • Minimálně jeden 10/100/1000 Mbps management port na každý Storage procesor
Další konektivita	Možnost rozšíření každého Storage procesoru o další volitelnou technologii: • 4port BE SAS 12Gbit • 1/10Gbit Tbase • 25Gbit SFP28 • 16/32Gbit FC
Monitoring / Správa	Monitoring diskového pole s možností sledování minimálně: • IOPS • MB/s pro front-end a back-end • Vytížení CPU a cache Správa a monitoring prostřednictvím HTML5 grafického uživatelského rozhraní i CLI Možnost správy a monitoringu jak přímo při připojení na Storage procesor, tak i přes aplikaci na serveru Možnost napojení do cloudového nástroje výrobce pro proaktivní monitoring celého systému.
Kompatibilita a podporované OS	• VMware vSphere 7x a 8x • Microsoft Windows Server 2019/2022 • Red Hat RHEL 7x a 8x • SUSE SLES 15x
Podpora a servis, doprava	podpora na 5 let, od nahlášení na podporu výrobce zařízení, technik na místě zahájí HW opravu do 4h, oprava v místě instalace, servis je poskytován výrobcem, jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému, možnost stažení ovladačů a management software na webových stránkách.

VAROVÁNÍ RIZIK TECHNOLOGIÍ SPOLEČNOSTI HUAWEI

V souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, v platném znění (dále jen „**ZKB**“), je zadavatel povinnou osobou, která musí provádět systematické hodnocení rizik spojených s technickými a programovými prostředky, jež jsou součástí její kritické infrastruktury.

Podle § 5 odst. 1 Vyhlášky č. 82/2018 Sb., v platném znění (dále jen „**VoKB**“) je zadavatel povinen provádět analýzu rizik a implementovat adekvátní bezpečnostní opatření. Tato analýza je nezbytná pro zajištění souladu s požadavky na kybernetickou bezpečnost a ochranu před potenciálními hrozbami, které mohou ohrozit integritu, důvěrnost a dostupnost informačních systémů.

Vzhledem k významu poptávaného plnění pro zajištění kybernetické bezpečnosti je dodavatel klasifikován jako významný dodavatel podle § 2 písm. n ZKB, což vyžaduje, aby zadavatel před uzavřením smlouvy posoudil rizika spojená s dodavatelem a jeho nabídkou. Dne 17. prosince 2018 vydal Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) varování č. j. 3012/2018-NÚKIB-E/110, které identifikuje technologie a programové prostředky společností Huawei Technologies Co., Ltd. a ZTE Corporation jako potenciální hrozby v oblasti kybernetické bezpečnosti. Toto varování je klíčovým dokumentem pro hodnocení rizik, neboť použití těchto technologií může představovat vysoké nebo kritické riziko pro informační bezpečnost a může vést k narušení důvěrnosti, integrity a dostupnosti dat. V rámci hodnocení rizik zadavatel zohlednil interní bezpečnostní dokumentaci, dosavadní poznatky o technickém stavu a relevantní legislativu, včetně návrhu nového zákona o kybernetické bezpečnosti, který transponuje Směrnici Evropského parlamentu a Rady 2022/255. V souladu s metodikou a podpůrným materiálem vydaným NÚKIB byla provedena aktuální analýza rizik, která prokázala, že rizika spojená s technologiemi Huawei a ZTE jsou pro zadavatele neakceptovatelná. V případě, že nedojde k legislativním nebo technickým změnám, zadavatel výslovně upozorňuje dodavatele, že mohou být vyloučeni ze zadávacího řízení, pokud jejich nabídka obsahuje technologie těchto společností. Na základě identifikovaných rizik a varování NÚKIB se zadavatel rozhodl nepřipouštět nabídky na technické a programové prostředky od společností Huawei a ZTE. Toto opatření je odůvodněno nejen varováním NÚKIB, ale také provedenou analýzou rizik, která ukazuje, že snížení rizika spojeného s používáním technologií těchto společností není možné dosáhnout jinak než jejich vyloučením z předmětu plnění veřejné zakázky. Zadavatel se zavazuje k dodržování všech povinností vyplývajících ze ZKB a k zajištění vysoké úrovně kybernetické bezpečnosti.

Vyloučení technologií od společností Huawei a ZTE je klíčovým krokem k ochraně před potenciálními hrozbami a zajištění bezpečnosti informačních systémů. Tímto způsobem se zadavatel snaží minimalizovat rizika a chránit svou infrastrukturu před kybernetickými útoky, čímž přispívá k celkové stabilitě a bezpečnosti kybernetického prostoru.