|  |
| --- |
| **Příloha č. 2: Technická specifikace** |

## Popis výchozího stavu

* + - 1. Současná ICT infrastruktura Základní škola Ostrava-Muglinov, Pěší 1/66, příspěvková organizace (dále jen škola nebo ZŠ) je tvořena mixem starších technologií pořízených a implementovaných v uplynulých letech. Jedná se především o jeden fyzický server, datové rozvody a většinu koncových stanic.
			2. Síťová infrastruktura
				1. **WAN** - škola je připojena do internetu přes poskytovatele OVA!!! CLOUD.net s rychlostí 20MBit/s na 20MBit/s

Připojení je realizováno bez veřejné IP adresy a využívá firewall, který je součástí dodávky služby od poskytovatele internetu

Škola má oddělenou privátní LAN síť od sítě poskytovatele internetu

Router D-LINK zajišťuje fyzické oddělení obou sítí

* + - * 1. **LAN** – pro rozvody vnitřní sítě jsou použity switche, které jsou od různých výrobců a pracují s rychlostí 100/1000Mb. Switche jsou bez administrace, nejsou napojené na UPS, nemají zálohované napájení 230V.

Přístupy na internetové stránky nejsou z vnitřní sítě školy nijak monitorovány, logovány ani řízeny a omezovány.

* + - * 1. **WIFI** - škola není nijak komplexně pokryta WiFi signálem
			1. Serverová infrastruktura
				1. Škola provozuje jeden server, na kterém jsou provozovány všechny systémy a aplikace
				2. Server je fyzicky umístěn v počítačové učebně v prvním patře budovy, dveře jsou opatřeny zámkem a nejsou zabezpečeny mříží. Přístup žáků do učebny je pouze v doprovodu vyučujícího.
				3. Server je opatřen CPU Intel E5300, RAM 8GB, HDD 500GB v režimu RAID 1
				4. Na serveru je provozován operační systém Windows Server 2008 R2, který je udržován aktualizovaný. Na serveru jsou nainstalované a zkonfigurované tyto serverové role:

Active directory

DHCP

DNS

FILE server

Webový server IIS

* + - * 1. Na serveru není použita žádná virtualizace prostředí
				2. Server je připojen na záložní zdroj UPS APC Smart 750 s možností administrace
			1. Provozovaný SW a využívané služby
				1. Emailové služby – všechny emailové schránky školy jsou umístěny mimo školní síť v externím hostingu - Best-Hosting.cz
				2. Webové stránky – webová prezentace školy je součástí hostingu u firmy Best-Hosting.cz . Stránky jsou provozovány na adrese www.zspesi.cz
				3. Antivirový systém - na všech koncových stanicích je nainstalován antivirový software Eset Endpoint Antivirus s centrálním managementem, který je nainstalovaný na školním serveru
				4. SW Bakaláři – software pro kompletní administrativu školy, dostupný na síťové složce serveru nebo pomocí webové aplikace pro všechny pedagogické pracovníky a vedení školy.
			2. Zálohování serveru je prováděno pomocí integrovaného nástroje Windows Server Backup, jako jediné medium pro uložení zálohovaných dat je použit externí USB harddisk s kapacitou 1 TB.
			3. Správci systémů jsou vyškoleni na správu provozního prostředí na bázi produktů Microsoft.

## Popis cílového stavu a specifikace předmětu plnění

### Základní požadavky na technické řešení

* + - 1. Cílem projektu je zvýšení bezpečnosti a související modernizace IT infrastruktury, aby implementací projektu byly naplněny Standardy konektivity škol [[1]](#footnote-1) (dále jen Standard konektivity) a rozšířena funkčnosti ICT prostředí Základní škola Ostrava-Muglinov, Pěší 1/66, p.o. podle Výzvy č. 46 Infrastruktura základních škol. Dílčí cíle dle jednotlivých komodit jsou specifikovány následovně:

| Označení  | Komodita  | Počet  |
| --- | --- | --- |
| K1  | Virtualizační platforma | 1 |
| K2  | Zabezpečení LAN a Wifi | 1 |
| K3  | Centrální logování | 1 |

* + - 1. Je požadováno řešení zachovávající a rozvíjející současné softwarové platformy Microsoft pro zachování kompatibility se stávajícími systémy a aplikacemi. Přechod na jinou platformu by způsobil uživatelské a provozní potíže.
			2. Pokud dodavatel vyžaduje využití konkrétních softwarových produktů a jím zvolený přístup k realizaci zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.
			3. Pokud dodavatelem nabízené řešení vyžaduje komponenty či služby neobsažené v požadavcích zadání, zahrne dodavatel do své ceny všechny náklady na jejich pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu, přičemž nesmí překročit předpokládanou hodnotu zakázky.
			4. Zadavatel z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů vyžaduje využití stávajících prostředků a používaných technologií. V případě, že dodavatel vyžaduje ve svém řešení stejné nebo podobné funkce, jaké poskytují stávající prostředky a technologie, je povinen využít nebo vhodným způsobem rozšířit stávající prostředky.
			5. Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky a dodavatel splnění těchto podmínek potvrdí samostatným čestným prohlášením:
				1. jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
				2. mají plnou záruku od výrobce,
				3. mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
				4. obsahují všechny nezbytné licence na používání příslušného softwaru,
				5. jsou v databázi výrobce uvedeny jako prodaná kupujícímu,
				6. jsou určeny pro provoz v České republice.

Tyto skutečnosti dodavatel doloží čestným prohlášením distributora, popř. čestným prohlášením dodavatele, nelze-li prohlášení distributora získat.

Zadavatel si vyhrazuje právo na zjištění původu výrobků při jejich předávání, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.

* + - 1. Veškerá dokumentace vytvořená v rámci realizace veřejné zakázky, musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. MS Office, Open Office, PDF) používaných zadavatelem na datovém nosiči a 1x v papírové formě. Struktura i forma dokumentace musí být před předáním předána ke kontrole a výslovně schválena zadavatelem.

### Specifické požadavky na technické řešení

* + - 1. **K1 - Virtualizační platforma**
				1. Pro provoz veškerých pořízených systémů a aplikací bude pořízen jeden server vybavený rychlým interním úložištěm s vysokou kapacitou. Hardware serveru bude virtualizován a na serveru bude možno provozovat několik virtuálních serverů. Server bude připojen do sítě duální optickou linkou 2x 10 Gb. Pořízený server musí být výrobcem určen pro provoz v běžném, neklimatizovaném prostředí do teploty 40 stupňů Celsia (krátkodobě až 45 stupňů Celsia) – např. dle ASHRAE Class A4.
				2. Pro zálohování bude v rámci projektu pořízeno síťové uložiště NAS s dostatečnou kapacitou pro ukládání provozních záloh a archivů logů monitorovacího a logovacího systému. Zálohování bude řízeno pokročilým zálohovacím software, který bude prostřednictvím virtualizačního hypervizoru zálohovat všechny virtuální servery. Zálohovací systém umožní zálohovat i fyzické servery a osobní počítače. Sítové úložiště NAS bude kvůli bezpečnému oddělení záloh od produkčních dat umístěno mimo místnost serveru – optimálně v zabezpečené, uzamykané místnosti v jiné budově, části budovy.
				3. Provozní zabezpečení bude tvořeno souborem non-IT technologií, které zajistí optimální podmínky pro spolehlivý chod technologií – především serveru:

Záložní zdroj napájení UPS zajistí chod serveru při výpadku napájení

Uzamykatelný rack zajistí bezpečné uložení serveru, správné větrání a zamezí neoprávněné manipulaci se serverem

* + - * 1. Pro zajištění bezpečnosti a možnosti řízení provozu v síti a zajištění prokazatelného monitoringu, logování a auditu interního i externího síťového provozu bude vybudována centrální databáze identit na bázi adresářové služby. Adresářová služby umožní ukládání a přehlednou správu identit (účtů včetně metadat) učitelů, žáků i externích subjektů, ale i technických prostředků – serverů, tiskáren, pracovních stanic apod. Adresářová služba bude poskytovat službu LDAP a umožní snadné napojení autentizačních mechanismů a protokolů – radius, agenta firewallu a dalších. Adresářová služba zajistí ověřování uživatelů pro účely jejich autorizace k přístupu k síťovým prostředkům (LAN, Internet atd.) i výpočetním zdrojům (pracovní stanice, tiskárny, sdílené složky atd.). Technické provedení bude založeno min. na 2 řadičích adresářové služby kvůli vysoké dostupnosti. Řadiče budou provozovány ve virtuálním prostředí a budou pravidelně automaticky zálohovány. Součástí řadičů budou základní síťové služby – DNS, DHCP, obě v konfiguraci pro vysokou dostupnost. Ověřování identit musí být dostupné i systémům, které přímo nepodporují LDAP nebo jiný protokol adresářové služby. Součástí projektu bude proto i vybudování tzv. zprostředkovatelů identit, které umožní ověřování i jinými protokoly. Technicky půjde o softwarové komponenty transformující požadavky na ověření identity do formátu akceptovaného adresářovou službou.
			1. **K2- Zabezpečení LAN a Wifi**
				1. Bude implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby s využitím technologie 802.1X.
				2. Pro hosty a externí uživatele bude zřízena samostatná VLAN (Guest VLAN), které bude komunikačně (min. L3 pravidla, ACL) oddělena od vnitřních sítí organizace. Tato VLAN bude mít své L3 rozhraní až na úrovní firewallu, tak aby bylo možné komunikaci podrobit kontrole za pomoci UTM nástrojů (min. AV, IPS, kategorizace obsahu) a mohl jí být přiřazen samostatný profil odlišný od profilů pro učitele a žáky. Ověřování přístupu do této VLAN bude zajištěno pomocí tzv. captive portálu – webové autorizace. Captive portál bude zajištěn firewallem případně jiným samostatným řešením nebo prvkem, ale vždy s důrazem na bezpečné oddělení uživatelského provozu od zbytku vnitřních sítí.
				3. Řízení provozu v LAN bude realizováno vytvořením VLAN (802.1Q), segmentací sítě s routováním (přepínáním) provozu mezi VLAN na úrovni centrálního přepínače s nastavitelnými ACL. Pro řízení provozu na úrovni kvality služeb bude k dispozici technologie QoS (Quality of Services). Pro zajištění vysoké výkonosti budou klíčové aktivní prvky propojeny opticky na rychlosti 10Gbit.
				4. Architektura WiFi bude založena na řešení s centrální správou prováděnou virtuálním kontrolerem (řadičem), který bude součástí firmwarů přístupových bodů a bude konfigurován v režimu vysoké dostupnosti a zajistí automatické rozložení zátěže klientů, roaming mezi spravovanými přístupovými body a automatické ladění kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení.
				5. Umístění pořízených AP bude provedeno na základě provedené analýzy pokrytí signálem pro zajištění konzistentní WiFi služby v pokrytých prostorách. Provedení analýzy bude součástí projektu.
				6. Ověřování přístupu do LAN bude realizováno protokolem 802.1X vůči adresářové službě prostřednictvím protokolů radius a P/EAP. V budoucnu pořizovaná zařízení (min. stolní i přenosné počítače) by měla být vybavena tzv. suplikantem - softwarovou komponentou, která dokáže předávat ověřovací požadavky síťovým prvkům, které tyto požadavky ověří vůči adresářové služby. Pro ověření zařízení bez suplikantů (např. starší tiskárny, zařízení na bázi jednoduchých operačních systémů či firmware apod.) bude použit jiný - dodavatelem navržený - vhodný způsob ověření. Neověřená zařízení nezískají přístup do sítě vůbec nebo jim bude zpřístupněna pouze VLAN s omezeným přístupem (např. Intranet). Spolu s ověřováním (autentizací) bude implementována i autorizace, tedy dynamické zařazení klientského zařízení nebo uživatele do určené VLAN.
				7. Ověřování přístupu do WiFi sítě bude realizováno na stejném principu jako LAN (tj. protokol 802.1X + radius). Wifi bude nabízet více SSID (učitelé, žáci, Guest), které budou obsluhovány samostatnými VLAN a budou napojeny na raduis servery. Učitelé a žáci budou prostřednictvím radius serveru ověřováni v adresářové službě. Zabezpečení vnitřních sítí (BSSID) školy bude provedeno dle 802.1i, tedy - WPA2 s AES šifrováním a konfigurováno shodně pro obě frekvenční pásma. Výjimkou bude síť určená výhradně pro hosty (Guest WiFi), kde bude realizován tzv. captive portál zajišťující webovou autentizaci hostů pomocí přidělených účtů nebo za pomoci před-generovaných číselných kupónů. Preferován bude captive portál firewallu s tzv. lobby přístupem pro správu a generování účtů/kupónů ne-technickou osobou.
			2. **K3 - Centrální logování**
				1. Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací - může jednat o jediné zařízení, softwarový nástroj či appliance. Řešení umožní správu z jedné grafické konzole, přístupné nativně skrze https bez nutnosti instalace klienta. Data bude ukládána do jedné databáze (nebo více integrovaných databází) tak, aby bylo možno realizovat multikriteriální vyhledávání napříč informacemi z různých zdrojů (např. přepínače/ netflow a firewall/syslog).
				2. Veškeré dále požadované informace si bude systém automaticky získávat, vyčítat z monitorovaných systémů a současně bude umožňovat příjem protokolů určených pro přenos logovacích, provozních informací, alertů a událostí. Systém bude přijímat informace standardními protokoly ze síťových a dalších aktivních zařízení a Windows server systémů.
				3. Mandatorní informace, která bude v systému vždy obsažena a uchována, je vazba IP-uživatel-čas. Tuto informaci bude systém čerpat ze security event-logu adresářové služby, dále z informací o probíhajících komunikacích prostřednictvím firewallu a dalších přístupových a autentifikačních systémů (např. radius logy). Dále budou získávány informace o překladu zdrojových, vnitřních IP adres na externím výstupním rozhraní firewallu, kde bude prováděn NAT. Bude se tedy jednat o informace obsažené v NAT tabulce. Spolu s tím musí být po stanovenou dobu možné zpětně dohledat i vnější provoz k vnitřnímu zařízení. Další funkcionalitou bude plnohodnotná práce se síťovými toky, jejich zpracování a archivace. Nástroje systému budou umožňovat i analytickou práci s přijímanými toky a to i zpětně.
				4. Kombinací požadavků Zákona o uchování informací v elektronické komunikaci spolu s požadavky Standardu konektivity škol a praktického pohledu na možné časové prodlení mezi vznikem incidentu a jeho vyšetřováním je definováno, že monitorovací a logovací systém bude umožňovat retenci dat min. 180 dnů. Na tento rozsah retence musí být dostatečně dimenzován, především z hlediska diskové kapacity, RAM i CPU, tak aby nedocházelo k výkonovým ani kapacitním problémům a systém měl dostatečnou rezervu pro očekávatelný budoucí nárůst informací a jejich zdrojů.

### Implementační služby

* + - 1. V rámci implementace předmětu plnění dodavatel realizuje pro všechny nabízené komodity K1 až K3 – následující služby:
				1. Provedení předimplementační analýzy (včetně plánovaných změn v konfiguraci současné infrastruktury) a zpracování detailního finálního popisu cílového stavu a postupu implementace. Výstupem bude prováděcí dokumentace, podle které bude dodavatel řešení implementovat. Prováděcí dokumentace musí být před zahájením implementace výslovně schválena zadavatelem. Prováděcí dokumentace musí respektovat a využívat osvědčené praktiky (tzv. Best Practice) a doporučení výrobců nabízených technologií.
				2. Dodávka a implementace předmětu plnění dle schválené prováděcí dokumentace včetně technické podpory.
				3. Zajištění projektového vedení realizace předmětu plnění.
				4. Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení popisu činností běžné údržby a činností pro spolehlivé zajištění provozu. Popis činností běžné údržby bude pokrývat minimálně následující oblasti:

Active Directory – správa uživatelů a skupin, zařazení počítače do domény

Zálohování – kontrola činnosti, obnova souborů

Hypervizor – ovládání virtuálních serverů, změna jejich konfigurace

Monitorovací a logovacího systém - vyhledávání činnosti uživatelů a systémů, běžná správa a kontrola funkce

LAN a Wifi - připojení zařízení vč. podrobných uživatelských postupů pro Wifi připojení mobilních zařízení (tablety, chytré telefony, notebooky) s operačními systémy Windows 7 a 10, Android, iOS a masOS.

Firewall – blokování stránek, dohledání činnosti uživatele, práce s kategoriemi stránek, zablokování přístupu pro uživatele skupinu

* + - * 1. Zpracování dokumentu Zásady využívání ICT a přístupu k síti dle Standardu konektivity pro začlenění do vnitřních předpisů školy.
				2. Zpracování materiálů pro školení a provedení školení v rozsahu dle kapitoly 2.4
				3. Zajištění zkušebního provozu infrastruktury v délce minimálně 2 týdnů včetně technické podpory specialistů na dané zařízení/službu s dostupností maximálně do 4 hodin na místě realizace od nahlášení požadavku v pracovní den v době od 8h do 17h.
				4. Provedení akceptačních testů.
				5. Předání do plného provozu.
			1. Činnost omezující práci uživatelů musí být prováděny primárně mimo běžnou pracovní dobu ZŠ, tj. mimo pracovní dny 7 – 15 hod. Ve výjimečných případech a po vzájemné dohodě Zadavatele a Dodavatele lze tyto práce provést i v pracovní době.
			2. Zadavatel dále požaduje provést minimálně následující implementační práce na dodaných komponentech a případně dalších zařízeních. Dodavatel je dále povinen zahrnout do nabídky veškeré další činnosti a prostředky, které jsou nezbytné pro provedení díla v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik, i v případě pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné.

|  |
| --- |
| K1: Virtualizační platforma |
| * 1. Návrh a kompletní implementace serverové virtualizační platformy
	2. Implementace pořízených technologií
	3. Analýza dat a systémů na stávajících serverech a jejich migrace na novou platformu
	4. Návrh vhodné struktury Active Directory s redundantními řadiči, její vybudování a migrace stávající
	5. Návrh a realizace zálohovacího řešení
	6. Implementace automatické odstávky a najetí serveru v případě výpadku a obnovení dodávky elektrické energie
	7. Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy
 |
| K2: Zabezpečení LAN a Wifi |
| * 1. Analýza stávajícího síťového prostředí a návrh nového architektury LAN i WiFi
	2. Implementace pořízených technologií
	3. Provedení segmentace LAN – VLAN, adresování, routování
	4. Zavedení IPv6 pro přístup k internetovým zdrojům publikovaným na IPv6 adresách
	5. Zavedení IPv6 pro veškeré publikované služby ZŠ z interních či externích prostředků. Včetně zajištění jednání a řízení změn u externích poskytovatelů služeb. Jde zejména o služby hostování domén http://zsbohuminska.cz/, DNS, e-mail, web školy, Bakaláři pro rodiče
	6. Zabezpečení komunikace publikovaných služeb ZŠ pomocí nabízeného certifikátu.
	7. Zavedení DNSSEC pro interní DNS služby i zabezpečení domén http://www.bohuminska.cz
	8. Návrh a implementace 802.1X pro kabelovou LAN i WiFi včetně uživatelské dokumentace pro konfigurace obvyklých zařízení a jejich systémů - PC, notebooky, chytré telefony, tablety, tiskárny - Windows, Linux, MacOS, Android, IOS, embedded systémy periferií
	9. Návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) pro školu
	10. Vybudování VPN pro vzdálený přístup uživatelů LAN na bázi webového portálu
	11. Respektování min. 3 různých skupinu uživatelů (učitelé, studenti, hosté) v návrzích a implementaci bezpečnostních a ostatních politik
	12. Implementace portálu pro registraci a řízení přístupů hostů – tzv. captive portál
	13. Instalace RACKů, vybudování optického propoje a vybudování LAN rozvodů k AP
	14. Zajištění ostatních nezbytných činností pro naplnění Standardu konektivity
 |
| K3: Centrální logování |
| * 1. Návrh a implementace systému pro centrální logování pro naplnění požadavků Standardu konektivity, především, ale nejen:
	+ monitoring a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení (ve spolupráci s firewallem)
	+ logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel, a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)
	+ monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) - RFC3954 nebo ekvivalent (např. netflow) – systém pro monitorování a sběr provozně - lokačních údajů minimálně na úrovni rozhraní WAN, ideálně i LAN) a to bez negativních vlivů na zátěž a propustnost zařízeni
	1. Provedení souvisejících konfigurací monitorovaných systémů
 |

* + - 1. Akceptační testy musí pro všechny komodity vždy zahrnovat minimálně prokázání kompletnosti dodávky a požadované funkčnosti. Návrh vhodných akceptačních kritérií bude součástí nabídky, zadavatel může v průběhu zpracování Předimplementační analýzy provést jejich upřesnění či rozšíření. Povinným akceptačním kritériem bude prokázání naplnění požadavků Standardu konektivity dle manuálu uveřejněného na <http://www.strukturalni-fondy.cz/cs/Microsites/IROP/Novinky/Zverejneni-doporucujiciho-manualu-k-postupum-pri-prokazani-a-kontrole> včetně úspěšného provedení a doložení testu na <https://www.standardkonektivity.cz/>. Prokázání naplnění požadavků poskytne dodavatel v písemné formě vhodné jako příloha k Závěrečné zprávě o realizaci projektu.
			2. Náklady na provedení implementačních služeb musí být zahrnuty v nabídkové ceně k položce (komoditě), ke které se vztahují a nelze je vyčíslit zvlášť.

### Školení

* + - 1. Dodavatel provede pro každou komoditu odborné školení na obsluhu a práci s dodanými zařízeními a to minimálně v rozsahu provozní dokumentace.
			2. Školení bude pokrývat všechna zařízení a systémy všech komodit, dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu:
				1. běžných administrátorských činností pro implementované systémy
				2. standardní údržby systémů pro administrátory zadavatele
			3. Školení dále zajistí seznámení pracovníků zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.
			4. Minimální rozsah školení pro každou komoditu jsou 2 hodiny (celkem min. 10 hod), není-li uvedeno jinak. Školení bude probíhat v sídle zadavatele. Předpokládá se účast max. 3 osob.

### Harmonogram projektu

* + - 1. Zadavatel vyžaduje dodržení následujícího harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro jednotlivé kritické milníky. Údaj D značí datum podpisu smlouvy o dílo. Čísla značí počet kalendářních dnů.

| Aktivita | Začátek | Termín |
| --- | --- | --- |
| Podpis smlouvy | D | D |
| Zahájení projektu – úvodní projektová schůzka | D | D+7 |
| Předimplementační analýza – zpracování | D+7 | D+12 |
| Předimplementační analýza – připomínkové řízení, schválení | D+12 | D+19 |
| Prováděcí dokumentace – zpracování | D+19 | D+33 |
| Prováděcí dokumentace – připomínkové řízení, schválení | D+33 | D+38 |
| Realizace předmětu plnění | D+38 | D+68 |
| Školení administrátorů | D+68 | D+73 |
| Zkušební provoz | D+73 | D+78 |
| Akceptační testy | D+78 | D+88 |
| Zahájení ostrého provozu | D+88 | - |
| Rezerva projektu |  | 10 |

* + - 1. Dodavatel může dle svého uvážení výše uvedené maximální lhůty trvání zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb.
			2. Maximální lhůty trvání nesmí dodavatel při tvorbě detailního harmonogramu prodloužit.
			3. Dodavatel uvede závazný harmonogram plnění ve své nabídce a zároveň v návrhu smlouvy.
			4. Dodavatel uvede potřebnou součinnost zadavatele pro splnění harmonogramu plnění ve své nabídce.
			5. Nejpozdější termín pro zahájení ostrého provozu a ukončení implementační fáze projektu je uvedena v Zadávací dokumentaci.

### Popis povinných parametrů dodávaného řešení

* + - 1. V dále uvedených tabulkách jsou uvedeny povinné parametry prvků nabízeného řešení. Dodavatel musí všechny parametry splnit, v případě nesplnění požadavku zadavatele bude nabídka dodavatele vyřazena a dodavatel bude následně vyloučen z účasti v zadávacím řízení.
			2. Dodavatel ve své nabídce detailně popíše způsob naplnění každého povinného parametru včetně značkové specifikace nabízených dodávek. Popis způsobu naplnění každého povinného parametru bude konkrétní, úplný a musí výslovně prokazovat, že nabízené řešení jednoznačně splňuje všechny aspekty povinného parametru.
			3. Dodavatel do tabulky povinných parametrů uvede odkaz na část nabídky, kde je možné ověřit naplnění parametru, tzn. na část nabídky s detailním popisem dle bodu (2). Vyplněné tabulky z tohoto oddílu technické specifikace učiní dodavatel součástí své nabídky.
			4. **Tabulka č. 1** - Povinné parametry pro Komoditu **K1 - Virtualizační platforma:**

| **Komodita K1 - Virtualizační platforma** |
| --- |
| **Část** | **Parametr** | **Popis povinného parametru** | **Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek** | **Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| **Server1x** | Provedení  | rackové provedení max. 1U včetně výsuvných kolejnic a montážního materiálu do racku |   |   |
| CPU | Minimálně 2x procesor osmi-jádrový (dohromady tedy min 16 jader). Výkon serveru dle <https://www.cpubenchmark.net> min. 14900 bodů ve výkonnostním testu dvouprocesorových systémů |   |   |
| RAM | 96 GB, min. 2666 MT/s |   |   |
| Rozšiřitelnost RAM | min. 700 GB bez výměny modulů |   |   |
| HDD | 8x 1,2TB, všechny SAS 12Gb 10000 ot/min |   |   |
| USB/SD | Duální SD nebo USB úložiště pro virtualizační platformu, min 8Gb. |  |  |
| RAID | SAS12Gb, RAID 5, zálohovaná write back cache min. 2GB |   |   |
| LAN | Minimálně LAN 2x10Gb SFP+ a 4x 1GbE RJ-45 s podporou virtualizace - VMware NetQueue, Microsoft VMQ. Podpora NIC partitioning (NPAR) a ISCSI offload |   |   |
| USB | min. 3 USB konektory - min. 1x verze 3.0, min. 1x umístění na čelním panelu s podporou bootování, min. 1x interní |   |   |
| Management | Servisní modul s možnosti samostatného přístupu po management síti, možnost vzdálené klávesnice, myši a obrazovky bez nutnosti běhu OS, možnost zapínat a vypínat server, možnost bootování se vzdáleného média. Vyhrazený LAN port, podpora http/s, ssh, SNMP, syslog. Okamžité a historické hodnoty teplot a napájení. Podpora vícefaktorového ověřování (autentizace) |   |   |
| Provoní podmínky | určen pro provoz v běžném neklimatizovaném prostředí do 40 (nárazově až 45) stupňů Celsia |   |   |
| Napájení | 2x napájecí zdroj, redundance, min. specifikace dle 80 PLUS https://cs.wikipedia.org/wiki/80\_Plus  |   |   |
| Management | Stavové informace na čelním panelu s výraznou indikací nestandardních a chybových provozní stavů či parametrů (min. napájení, teplota, vada HDD. Aktivní indikace standardního provozního stavu.  |   |   |
| Záruka | min. 60 měsíců zajištěná výrobcem, v místě instalace v režimu 24x7 s reakční dobou 4 hodiny |   |   |
| **SW licenceoperačních systémů**  | Serverové operační systémy | 3 ks licencí 64-bitového serverového operačního systému v aktuální verzi. Každá licence musí umožnit provoz hypervizoru a min. 2 virtuálních serverů stejné verze v prostředí nabízené serverové virtualizace, dále provoz všech nabízených aplikací a management nástrojů. |   |   |
| Klientské licence | klientské licence pro nabízené operační systémy umožňující využívat těchto systémů 60 uživatelům |   |   |
| **SW licence pro serverovou virtualizaci** | Serverová virtualizace | Software pro virtualizaci serverů včetně management konzole musí licenčně pokrývat použití pro 6 fyzických procesorů ( 3 fyzické servery, každý max. dva procesory ) |  |  |
| Podpora zálohování | Funkcionalita, která bude provádět diskovou zálohu a jednoduchou obnovu na úrovni image virtuálních strojů nebo jednotlivých souborů |  |  |
| Správa a podpora |  Komplexní správa virtuální infrastruktury z jedné konzole a umožňující integraci s produkty třetích stranSoftware s podporou 5let |  |  |
| Podporované OS | Podpora operačních systémů Windows 2000 a novější, Linux, FreeBSD jako OS ve virtuálních strojíc |  |  |
| **UPS1x** | Provedení | Provedení do racku, max. 2U, včetně montážního materiálu |   |   |
| Elektrické provedení | Jmenovité́ napětí́ 230 V, jednofázová na vstupu i výstupu |   |   |
| Výkon (VA/W) | 1500 VA / 1350 W |   |   |
| Technologie | Line- interaktivní |   |   |
| Účinnost | Min. 95%, účiník 0,9 |   |   |
| Stabilizace | Výstupní napětí́ – odchylka max. ±10 % od jmenovité́ hodnoty |   |   |
| Kapacita | Doba běhu na baterie min. 10 min při 50% zátěži |   |   |
| Vstup | Zásuvka IEC C14 (16 A) |   |   |
| Výstupy | Min. 8 zásuvek IEC C13 s měřením spotřeby |   |   |
| Napájecí segmenty | Min. 2 nezávisle ovládané napájecí segmenty pro postupný náběh napájených technologií |   |   |
| Diagnostika | Vestavěný úplný́ systémový́ autotest, možnost automatického plánovaného provádění |   |   |
| Servis | Baterie musí být vyměnitelné za chodu, aniž by bylo nutné odstavovat připojená zařízení. |   |   |
| Bypass | Automatický interní bypass |   |   |
| Komunikační porty | RS-232, USB, vzdálené zapnutí/vypnutí, LAN management port |   |   |
| Stavové informace | Stavový grafický displej pro konfiguraci a základní informace o stavu UPS |   |   |
| Řízení | Schopnost ovládání a restartování nabízeného serveru, korektní shutdown operačních systémů |   |   |
| SW kompatibilita | UPS musí být plně podporovaná výrobcem pro použití ve virtualizačních prostředích VMware a Microsoft Hyper-V, příslušný SW bude součástí dodávky |   |   |
| Záruka | min. 36 měsíců (min. 24 na baterie) |   |   |
| **SW licence zálohovací software** | Licence | Licence zálohovacího software pro nabízený server bez omezení počtu zálohovaných virtuálních serverů a objemu dat. |   |   |
| Efektivita ukládání dat | Integrované technologie komprimace a deduplikace. |   |   |
| Nároky na správu | „bezagentové“ řešení – bez instalace agentů do zálohovaných virtuálních serverů či aplikací |   |   |
| Ochrana dat | provádění datově konzistentních záloh hlavních serverových aplikací – Microsoft SQL server, Active Directory, souborové systémy – bez nutnosti odstávky aplikace |   |   |
| Fyzické servery | Vestavěná podpora zálohování stávajících fyzických serverů - pro fyzické servery je přípustné využívat agenty |   |   |
| Podpora WAN | možnost plnohodnotné replikace přes WAN pro replikaci virtuálních serverů do vzdálených lokalit (např. Technologického centra Plzeňského kraje) |   |   |
| Snapshoty | využívání snapshotů, zálohování pouze dat změněných od poslední úspěšné zálohy |   |   |
| Kompatibilita | podpora operačních systémů Windows a Linux v zálohovaných virtuálních serverech |   |   |
| Uložiště záloh | Možnost ukládání záloh na diskový prostor a páskovou jednotku/knihovnu |   |   |
| Fyzické servery | Podpora ukládání záloh nevirtualizovaných serverů a PC do společného úložiště a monitorování zálohovacích úl |   |   |
| Správa | vytváření a správa úloh (zálohování, obnova apod.) pomocí vestavěných průvodců včetně konfigurace automatického spouštění úloh |   |   |
| Správa | automatický reporting úspěšných i neúspěšných úloh |   |   |
| Správa | Běžné úlohy obnovy (obnovení souboru, databáze SQL, objekty Active Directory) provádět pomocí průvodců. |   |   |
| Záruka | min. 12 měsíců včetně opravných a funkčních aktualizací |   |   |
| **Síťové úložiště NAS1 ks** | Provedení | samostatně stojící, možno umístit i mimo rack |   |   |
| Výkon | CPU architektura 64 bit, min, 4 jádra |   |   |
| HDD | Min. 8 pozice pro HDD, rozšiřitelné min na 18 HDD |   |   |
| Rozšiřitelnost | Podpora připojení externích disků přes USB 3.0 (min. 4 porty) |   |   |
| Hot-swap | Disky vyměnitelné za chodu. |   |   |
| SSD HDD | podpora SSD disků pro ukládání dat i akceleraci rotačních HDD |   |   |
| Kapacita | Osazeno min. 8x 4TB  HDD SATAIII/64MB cache určených výrobcem pro NAS (nepřipouští se HDD určené jiným účelům (desktop, kamerové systémy apod.). |   |   |
| Konektivita | Min. 4 x 1GBit Ethernet porty s podporou agregace linek a redundance. |   |   |
| Výkon | Přenos souborů v systému Windows, SMB, 1Gbit, zápis min. 60MB/s |   |   |
| Kompatibilita | Plná podpora Microsoft Hyper-V a Windows ADS a ACL. |   |   |
| Komunikace LAN | Síťové protokoly CIFS, WebDAV, iSCSI, SSH, SNMP, http/s |   |   |
| UPS | Podpora korektního vypnutí signálem z UPS přes LAN při výpadku napájení |   |   |
| RAM | min. 8GB DDR3 |   |   |
| Ochrana dat | Integrované typy ochrany dat RAID 1, RAID 5, RAID 6, RAID 10 |   |   |
| Záruka | min. 36 měsíců včetně HDD |   |   |

* + - 1. **Tabulka č. 2** - Povinné parametry pro Komoditu **K2 – Zabezpečení LAN a Wifi**:

| **Komodita K2 - Zabezpečení LAN a Wifi** |
| --- |
| **Část** | **Parametr** | **Popis povinného parametru** | **Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek** | **Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| **Firewall1x** | Porty | min 10x 1GbE (min. 2x WAN), USB pro ext. modem |   |   |
| Propustnost | min. 3 Gbps pro libovolnou velikost paketu |   |   |
| Počet současných spojení | min. 1,2 miliónu |   |   |
| Propustnost SSL VPN | min. 150 Mbps, při licenčním nebo technickém omezení počtu klientů požadujeme min. 25 klientů |   |   |
| Propustnost IPS | min. 1.3 Gbps (HTTP) |   |   |
| Propustnost SSL inspekce | min. 170 Mbps |   |   |
| Kombinovaná propustnost | Firewall - sktivní IPS + aplikační kontrola + antimalware min. 200 Mbps pro běžný provoz |   |   |
| Virtualizace | min. 8 virtuálních kontextů |   |   |
| Vysoká dostupnost | režimy Active/Passive i Active/Active se společnou konfigurací |   |   |
| Dualstack | podpora současného běhu IPv4 a IPv6 |   |   |
| Aplikační kontrola | detekce, monitoring, povolení či zakázání obvyklých síťových aplikací na základě signatury dané aplikace, nikoliv dle portuKontrola komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S,…) |   |   |
| Antivir | Antivirus pro vybrané protokoly, možnost volby různých databází, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV engine, možnost detekce tzv. Grayware (rootkit, malware, spywave, keylogger, atd) |   |   |
| Kategorizace a blokace provozu | založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorii na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne |   |   |
| Antispam | antispamová a antivirová inspekce elektronické pošty |   |   |
| Bezpečnost | automatická aktualizace UTM funkcí poskytovaná výrobcem zařízení |   |   |
| Ověřování uživatelů | LDAP, Active Directory, Single Sign On vůči Active Directory, Radius, TACACS+, Ověřování na základě certifikátu |   |   |
| Management a monitoring | HTTP/S, SSH, SNMP, syslog,  |   |   |
| Sledování toků | export síťových toků (Netflow nebo ekvivalent) |   |   |
| Standardní funkce | NAT, statické a dynamické routování, publikace interních serverů |   |   |
| Záruka  | min. 60 měsíců v režimu 24x7. Odeslání náhradního zařízení max. následující den po nahlášení závady, včetně nároku na bezpečnostní aktualizace firmware a UTM (URL filtrace, IPS, antimalvare, antispam, aplikační kontrola) |   |   |
| **Centrální přepínač** | Základní parametry | L2/L3 přepínač v rackovém provedení max. 1U |   |   |
| Porty | 24x 1 GbE, 4x 10Gb SFP+ |   |   |
| Propustnost | neblokovaná architektura, propustnost min. 200 Gb |   |   |
| Rozšiřitelnost | možnost rozšíření počtu portů interním modulem - buď 15 portů 1Gb (volitelně metelické nebo SFP) nebo 4 porty 10 Gb SFP+ |   |   |
| Agregace portů | podpora LACP |  |   |
| Směrování | statické a dynamické routování, policy based routing |   |   |
| Řízení provozu | víceúrovňový QoS |   |   |
| VLAN | VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření |   |   |
| Ověřování uživatelů a zařízení | podpora 802.1X |   |   |
| Dualstack | plný IPv4 a IPv6 dualstack včetně směrování a QoS |   |   |
| Pokročilé funkce | podpora MPLS a VPLS včetně L2 a L3 MPLS VPN |   |   |
| Stohování  | pokročilé stohování - 2 (a více) přepínačů ve stohu se chovají jako jeden z pohledu správy i připojených zařízení |   |   |
| Sledování toků | export síťových toků (Netflow nebo ekvivalent) |   |   |
| Monitoring a správa | plná podpora CLI, SSH, SNMP 1-3, syslog, sFlow, RMON, web rozhraní |   |   |
| Záruka  | min. 60 měsíců v režimu 24x7, odeslání náhradního zařízení max. následující pracovní den po nahlášení závady, včetně nároku na opravné verze firmware |   |   |
| **Přístupové přepínače5ks** | **Společné parametry** |   |   |
| Základní parametry | Základní L3 přepínač v rackovém provedení max. 1U |   |   |
| Stohování  | podpora stohování pro jednotný management (přepínače musí stohovatelné vzájemně bez ohledu na provedení - viz. Porty a propustnost), min. 4 ks ve stohu |   |   |
| Propustnost | neblokovaná architektura |   |   |
| Agregace portů | podpora LACP |   |   |
| Dualstack | IPv4 a IPv6 dualstack včetně podpory ACL a QoS |   |   |
| VLAN | VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření |   |   |
| Ověřování uživatelů a zařízení | podpora 802.1X |   |   |
| Monitoring a správa | plná podpora CLI, SSH, SNMP 1-3, syslog, sFlow, RMON, web rozhraní |   |   |
| Záruka  | min. 60 měsíců v režimu 24x7, odeslání náhradního zařízení max. následující pracovní den po nahlášení závady, včetně nároku na opravné verze firmware |   |   |
| **Specifické parametry** |   |   |
| Porty a kapacita switchování | 1 kus - 8x 1 GB RJ-45 + 2x 10Gb SFP+, min. 55 Gbps4 kusy - 24x 1 GB RJ-45 PoE+ + 4x 1Gb SFP, min. 120 Gbps |   |   |
| **WiFi přístupové body (AP)13 ks** | Základní funkce | Přístupový bod (AP) WiFi včetně montážního materiálu na stěnu nebo strop |   |   |
| Frekvence | činnost v radiovém pásmu 2,4 a 5 GHz současně, 2 radiové moduly |   |   |
| Anténní systém | interní systém min. MIMO 3x3 (5 GHz) a MIMO 2x2 (2,4 GHz), optimalizovaný pro montáž na strop |   |   |
| Přenosové rychlosti | SU-MIMO (5GHz) až 1300Mbps, MU-MIMO až 867Mbps. 2,4GHz MIMO až 300Mbps.  |   |   |
| Standardy | podpora 802.3at, 802.11n, 802.11ac, 802.1x včetně přiřazování do VLAN |   |   |
| Řízení klientů | automatické směrování komunikace klientů z 2.4 GHz na 5 GHz (pokud klienti podporují obě pásma) |   |   |
| Rušení | průběžná detekce non-WiFi rušení a spektrální analýza |   |   |
| Multi SSID | podpora vysílání min. 8 SSID (WiFi sítí) současně, podpora přiřazení každého SSID samostatné VLAN |   |   |
| Zatížení |  min. 250 přiřazených (asociovaných) klientů na radiový modul |   |   |
| Porty | min. 1x 1Gb, PoE s podporou standardů 802.3at a 802.3af |   |   |
| Úsporné napájení | podpora standardu 802.3az - Energy-Efficient Ethernet (EEE) |   |   |
| Řízení provozu | klasifikace a kontrola provozu, detekce obvyklých aplikací s možností určení priority nebo šířky pásma zvoleného provozu |   |   |
| Řízení kvality služeb | automatické řízení kvality služeb (QoS) pro hlas a video |   |   |
| Současná obsluha více klientů | Podpora MU-MIMO (Multi-User MIMO) - multi-user multiple input/multiple output |   |   |
| Přenosové rychlosti | SU-MIMO (Single-User MIMO) min. 1300Mb, MU-MIMO min. 850 Mb  |   |   |
| Bezpečnost | Detekce cizích přístupových bodů zjištěných v LAN i v radiofrekvenčním pásmu |   |   |
| Virtuální kontroler | Virtuální, vysoce dostupný kontroler obsažený ve firmware každého přístupového bodu. Umožňuje kompletní centrální správu WiFi infrastruktury a řízení jejího provozu včetně roamingu klientů. |   |   |
| Monitoring a správa | plná podpora CLI, SSH, SNMP 1-3, syslog, web rozhraní |   |   |
| Správa frekvenčního pásma | automatické dynamické přidělování kanálů a řízení výkonu přístupových bodů pro vyrovnané pokrytí a minimalizaci interference |   |   |
| Záruka  | min. 60 měsíců v režimu 24x7, odeslání náhradního zařízení max. následující pracovní den po nahlášení závady, včetně nároku na opravné verze firmware |   |   |
| **Bezpečnostní certifikát** | Popis | Hvězdičkový (tzv. wildcard) certifikát veřejné certifikační autority pro zabezpečení služeb publikovaných do internetu. Kořenový certifikát certifikační autority musí být standardně obsažen v běžných desktopových a mobilních operačních systémech a být automaticky aktualizován v rámci aktualizace operačního systému.  |   |   |
| Záruka  | min. 36 měsíců |   |   |
| **Kabelové rozvody včetně příslušenství** | Racková skříň | Stojanová skříň pro umístění ICT techniky o rozměru 19“, výška 27RU, vnější rozměr 600x1000mm, perforované dveře s propustností min. 80%, uzamykatelné dveře i boční panely, horní a dolní prostupy/kanály pro vnější kabely |   |   |
| montážní materiál | Sada montážního materiálu pro dodanou rackouvou skříň, min. 50ks |  |  |
| Patch panel | Rack bude osazen 19'' modulárním patch panel 24portový 1U celokovový černý CAT6 (včetně modulů) |  |  |
| Nástěnný rozvaděč | Nástěnný rozvaděč min. 15U (š)600x(h)595, vylamovací záslepky pro montáž chladících jednotek nebo ventilátorů, dveře celoskleněné s bezpečnostním tvrzeným sklem 4 mm a zámkem |  |  |
| Police do rozvaděče | polička perforovaná 1U/450mm, nosnost min 70kg,integrované podpěry, montážní materiál |  |  |
| Záložní zdroj napájení | Pro ochranu napájení zařízení v nástěnném racku, vysokofrekvenční line interaktiv technologie, čistě sinusový výstup, zátěž min. 750VA/525W, vstup 1x IEC-320-C14, výstup min. 6x IEC-320-C13, tolerance vstupního napětí min. 184V – 276V, informační stavový LCD panel, min. 1x USB port a 1xRS232 sériový port |  |  |
| Optický propoj SM | 200m dlouhý optický spoj, kabel min 4 vlákna SM 9/125 OS2 LSOH, délka 200m, instalovaný v lištách, zakončený na obou stranách v 19" rozvaděči optickou výsuvnou vanou 1U, optická kazeta pro 2 x 8 svaru s víkem a držáky svaru, konektory LC, 4ks optický patch kabel LC-LC Duplex 9/125 OS1 2m, po instalaci bude provedeno měření trasy s protokolem o výsledku |  |  |
| LAN připojení AP WiFi13ks | Pro 13 ks poptávaných AP bude vybudován LAN Cat6 přívod, jenž bude zakončen na jedné straně zásuvkou RJ45 umístěnou na zdi nebo stropě, a na druhé straně v patch panelu. Kabel bude veden v elektroinstalační liště a nebude v průměru delší jak 50m. Každý vybudovaný přívod bude změřena a bude od něj měřící protokol. |  |  |
| Záruka  | Kabelové rozvody 10 let, rozvaděč a UPS 24 měsíců |   |   |

Součástí dodávky síťových prvků budou všechny potřebné metalické i optické patch kabely, potřebné SFP či SFP+ transceivery nebo DAC kabely.

* + - 1. **Tabulka č. 3** - Povinné parametry pro Komoditu **K3 – Centrální logování**:

| **Komodita K3 - Centrální logování** |
| --- |
| **Část** | **Parametr** | **Popis povinného parametru** | **Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek** | **Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| **Monitorovací a logovací systém1x** | Základní funkce | Systém pro sběr, ukládání a správu provozních a bezpečnostních informací a událostí ze sledovaných systémů  |   |   |
| Protokoly sběru logů | syslog, TCP, UDP, HTTP, AMQP, JSON |   |   |
| Sběr síťových toků | netflow či kompatibilní dle nabízeného firewallu a centrálního přepínače |   |   |
| Zdroje logů | Min. REST API, textové soubory, Radius, Active Directory, MS SQL databáze, Windows Event Log - včetně rozšířených "Applications and Services Logs", síťové prvky - syslog a netflow, ostatní aktivní prvky - syslog, SNMP trap  |   |   |
| Parsování logů | Integrovaný nástroj pro parsování logů. Možnost nahrání části logu, online vytváření parseru a snadné testování výsledku. Podpora vytváření opakovaně použitelných vzorků - např. definice IP adresy regulárním dotazem apod. |   |   |
| Retence | Uchovávání logů min. 6 měsíců, automatická retence logů a indexů |   |   |
| Geolokace | Podpora automatické doplňování logů o informaci o lokalitě podle IP adresy |   |   |
| Normalizace logů | Sjednocení názvů shodných dat z různých zdrojů logů např. pro snadné vyhledávání napříč zdroji |   |   |
| Rozšíření logů | Podpora rozšíření logů o vlastní statické a dynamické (kalkulované) položky integrovaným nástrojem. |   |   |
| Rozšiřitelnost | Podpora snadného rozšíření funkčnosti pomocí plug-inů nebo modulů |   |   |
| Bezpečnost | Podpora šifrované komunikace se zdroji (SSL apod.), ověřování zdrojů (TLS apod.) |   |   |
| Výkon | Min. 500 EPS (event per second), 5000 FPM (flows per minute) |   |   |
| Dashboardy | Uživatelské vytváření dashboardů (pracovních desek) včetně možnosti využití grafických prvků (grafy, mapy, histogramy apod.) i strukturovaných dat (tabulek) |   |   |
| Export dat | Export dat do csv a/nebo xls - min. výsledky hledání  |   |   |
| Kanály  | Možnost vytváření kanálů - datových sad či toků - na základě pravidel (logických podmínek) a to i napříč různými zdroji. Podpora dalšího zpracování - tvorba alarmů, zobrazení na dashboardu, online odesílání do nadřazeného systému apod.  |   |   |
| Alerty, notifikace | Podpora vytváření alertů - překročení okamžitých či kumulovaných hodnot, zasílaní upozornění |   |   |
| Active Directory | integrace s Active Directory pro ověřování uživatelů, nastavení oprávnění min. administrátor a operátor |   |   |
| Vyhledávání | Rychlé a intuitivní vyhledávání v záznamech napříč všemi zdroji i při velkých objemech dat (řády TB). Jednoduchý dotazovací jazyk. Rychlá vyhledávání či filtrování bez tvorby dotazů - např. výběrem v kontextovém menu vybraného pole uloženého záznamu. |   |   |
| Ovládání | Intuitivní grafické rozhraní  |   |   |
| Kompatibilita | Podpora provozu v prostředí nabízené serverové virtualizace |   |   |
| Ukládání dat | do databáze, případná databázová licence musí být součástí dodávky |   |   |
| Výstupy | Možnost výstupů do nadřazeného systému pro účely vzdáleného expertního dohledu. Zabezpečený přenos vhodným protokolem |   |   |
| Záruka | min. 60 měsíců včetně poskytnutí opravných verzí |   |   |

## Záruky a servisní podmínky

### Požadavky na záruky a servisní podmínky

* + - 1. Zadavatel uvádí u jednotlivých komodit požadovanou min. záruku, popř. podporu. Uváděné parametry byly průzkumem trhu zjištěny jako standardní, tj. poskytovány výrobci jako součást standardní dodávky a ceny.

Z důvodu zajištění udržitelnosti projektu a zajištění bezpečnosti provozu po dobu 60-ti měsíců požaduje zadavatel poskytnutí prodloužených záruk pro:

* server (součást K1)
* firewall (součást K2)

při zachování ostatních parametrů původní záruky (rychlost opravy, rozsah aktualizací firmware apod.). Cenu tohoto prodloužení zahrne dodavatel v Příloze 3 - Kalkulace nabídkové ceny, v nichž má být cena prodloužené záruky uhrazena.

* + - 1. Zadavatel požaduje bezplatný (zahrnutý v ceně zakázky) přístup k aktualizacím software a firmware dodaných komodit minimálně po dobu záruky.
			2. Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro zadavatele.
			3. Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.
			4. Není-li uvedeno u konkrétní komodity jinak, požaduje zadavatel provedení záruční opravy do pěti pracovních dnů
			5. Po dobu 60-ti měsíců od předání díla jako celku do plného provozu, musí dodavatel nebo výrobce všech zařízení garantovat běžnou dostupnost náhradních komponentů a dostupnost servisu.
			6. Dodavatel ve své nabídce výslovně uvede všechny podmínky záruk.
			7. Pro hlášení servisní požadavků zajistí dodavatel zhotoviteli přístup ke svému helpdeskovému systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení. Detailní popis helpdeskového systému a jeho obsluhy musí být součástí nabídky. Provozní doba helpdeskového systému musí být minimálně 7-17 hod. v pracovních dnech.
1. Viz. aktuální verze na <http://www.dotaceeu.cz/getmedia/85d2cb71-a58d-4d81-a6af-06d32999247f/Specificka-pravidla-46-vyzvy_ZS_1-5.pdf?ext=.pdf> a dále příloha P9 - Standard konektivity základních škol [↑](#footnote-ref-1)