1 Technická specifikace zadavatele (kupujícího)

Zadavatel požaduje dodávku jednotlivých komponent dle této technické dokumentace včetně příslušenství v níže uvedené minimální specifikaci.
Musí se jednat o zařízení nová, nepoužitá, nerepasovaná a určená pro prodej v České republice.
Součástí dodávky níže uvedených technologií budou i dále uvedené služby.
Součástí dodávky bude dále dodávka dokumentace a nezbytné zaškolení administrátorů v prostředí kupujícího k běžnému provozu a ovládání dodaných technologií včetně specifik a konfigurace provedené v prostředí kupujícího.
Nabízené zboží musí být standardní, běžně dostupné a určené k produkčnímu použití.
Není dovoleno použití beta-verzí, kódu s custom úpravami či neoficiálních verzí.
Veškeré nabízené zboží musí být pokryto oficiálním supportem, přičemž požadavek na provedení bezplatného servisního zásahu musí být možné kdykoliv vznést přímo na výrobce zařízení.
Veškeré deklarované funkce a technické parametry nabízeného zboží musí být dostupné nejpozději dnem podání nabídky.
Deklarované funkce a technické parametry nabízeného zboží musí být ověřitelné prostřednictvím oficiálních datasheetů, release notes či manuálů vydaných výrobcem.
Užité pojmy níže:

- NBD – další pracovní den, tzn. například realizace opravy zařízení nejpozději další pracovní den od nahlášení
- x BD – x pracovních dnů, tzn. například realizace opravy zařízení nejpozději poslední pracovní den dané lhůty od nahlášení
- on-site – realizace například opravy zařízení v místě dodávky

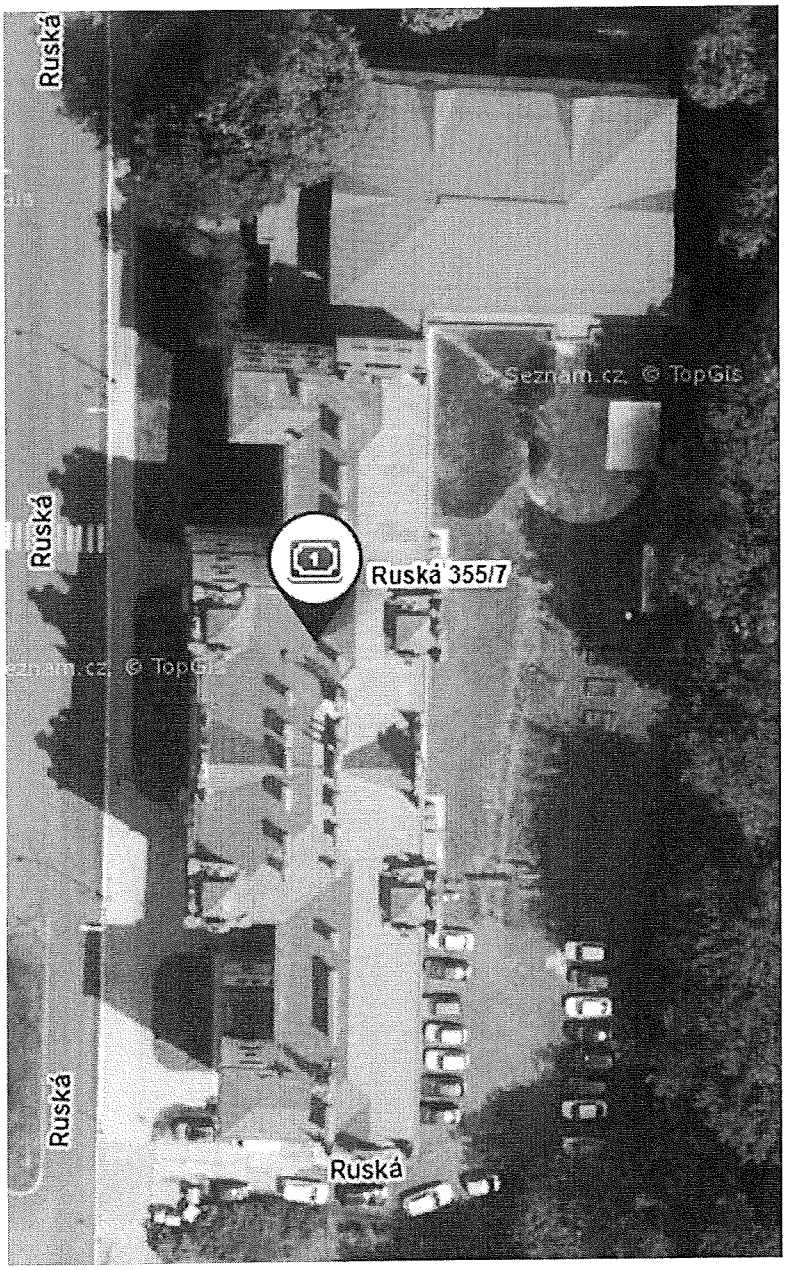
Propojení zařízení – SFP moduly a kabely
Všechny dodané technologie musejí být v rámci dodávky propojeny odpovídajícím způsobem a technologií, tedy zejména pro všechny síťové karty jednotlivých zařízení musejí být dodány i SFP a obdobné moduly a kabely do serverovny kupujícího, které takové propojení v kvalitě požadované u každého ze zařízení umožní. V případě 10Gbit karet musí být dodány SFP prvky a kabely umožňující využití této maximální rychlosti karty, v případě jiných rychlostí toto pravidlo musí být dodrženo stejně.

Počty jednotlivých komponent, které jsou předmětem tohoto plnění jsou uvedeny v samostatném souboru s názvem „Cenová tabulka".

Obsah

2 Popis současného stavu

(1) Areál Gymnázia a obchodní akademie Mariánské Lázně, příspěvkové organizace je umístěn na adrese Ruská 355/7, 35301 Mariánské Lázně a je tvořen hlavní budovou školy a přístavkem s tělocvičnou, viz. obrázek. V současné době navštěvuje školu téměř 430 žáků a škola má 47 zaměstnanců.



(2) Realizace plnění bude probíhat ve všech využívaných objektech.

(3) Současný stav ICT školy neodpovídá Standardu konektivity škol (dále jen Standard konektivity), a současným nárokům na výkon, bezpečnost a centralizovanou správu počítačové sítě. Počítačová síť byla budována postupně, staří a technické úroveň používaných prvků se výrazně liší. Síťové pokrytí na úrovni metalických kabelů Cat5 bylo budováno a rozšiřováno postupně podle aktuálních potřeb a finančních prostředků školy. Bezdrátové připojení bylo realizováno v roce 2021 na úrovni standardu

WiFi 5 pro potřeby pokrytí aktuálních potřeb a s ohledem na omezené finanční možnosti, bez rezerv pro budoucí rozvoj. Část použitých aktivních prvků sítě je již technicky i morálně zastaralých a výrobci nepodporovaných (nebo jen omezeně). Chybí významná provázanost a centralizovaná správa infrastruktury.

(4) Kabelové rozvody byly provedeny kabely Cat5e. Pokrytí potřebných prostor budov metalickými rozvody je nedostatečné a neumožňuje připojovat do sítě další zařízení (koncová zařízení, IoT a bezpečností prvky (kamery apod.) a síť rozvíjet např. doplňováním WiFi přístupových bodů. Nedostatek přípojných míst je na některých místech řešen „rozbočováním" sítě malými přepínači bez managementu, jejichž použití dále komplikuje správu celé sítě a snižuje její robustnost, stabilitu a bezpečnost. Kabeláž je uložena převážně v lištám, občas „pod kobercem".

(5) Aktuálně využívaný server byl dodán v roce 2020/09. Výkonem a kapacitou server vyhovuje aktuálním požadavkům, ale není schopen splnit všechny požadavky systému splňujícího požadavky Standardu konektivity.

(6) Server je aktuálně připojen rychlostí 10Git/s do páteřního switche ve spodním rozvaděči.

(7) V hlavní budově je umístěn další páteřní switch a propojení dvou páteřních switchů je provedeno optickým kabelem rychlostí 10Gbit/s. Optický kabel mezi spodním rozvaděčem (u tělocvičny) a horním rozvaděčem (učebna 316) je aktuálně veden nepoužívaným komínovým průduchem.

(8) Propojení stanic i serverů je zajištěno přepínači 1 Gb/s bez možnosti pokročilé správy. Hlavní aktivní prvky jsou umístěné v několika datových rozvaděčích. Aktivní prvky nesplňují požadavky na zabezpečení přístupu do LAN pomocí 802.1X.

(9) Internetové připojení je realizováno společností ČezNet optickým přípojem s rychlostí 200Mb/s symetricky včetně IPv6 konektivity. Rychlost připojení tak převyšuje požadavek Standardu konektivity škol – 107,5 Mbps (430 žáků x 0,25 Mbps).

(10) Škola má přiděleny veřejné IP adresy IPv4 (7 adres), včetně IPv6 veřejných adres s rozsahem :/ 56 adresy. Škola nemá v současné době validující DNSSEC resolver na straně školy, neprovádí pokročilý monitoring provozu. Škola provozuje 2 domény – goaml.cz a goaml.eu

(11) Škola provozuje Wifi síť, které pokrývá pouze část školy. Byla realizovaná v roce 2021 a splňuje technologické požadavky kategorie WiFi 5. Tato WiFi síť slouží pro potřeby zaměstnanců i žáků školy. Síť má více SSID. Síť pro zaměstnance školy je chráněná silným heslem a má přístup k systémovým prostředkům školy. Síť pro žáky je chráněna heslem a uživatelé této sítě mají povolený pouze přístup do internetu. Síť je centrálně spravovaná. Použité prvky nepodporují aktuální bezpečnostní standardy (WPA3 apod.), ani pokročilé funkce optimalizace rádiového provozu a obsluhy připojených klientů.

(12) Zabezpečení přístupu k internetu využívá pouze NAT na hraničním prvku – routeru. Nejsou využívány pokročilé bezpečnostní funkce např. URL filtrace, antivirová kontrolou a detekce průniků.

(13) Škola provozuje jeden fyzický server s virtualizací. Jako hypervisor pro virtualizaci se používá řešení VMWare 6.5 Je provozováno několik různorodých operačních systémů. Virtuální Windows server 2019 je využíván 4x pro Active Directory a sdílení souborů (zajišťuje DNS v síti), Bakaláře, Terminál server, a server Docházky. Na serverech jsou dále provozovány 3 virtuální Servery Linux v různých verzích - jednak pro webové stránky školy a různé projekty, dále pak pro odesílání mailů ze starších tiskových zařízení, které nepodporují dvoufaktorové ověřování a v neposlední řadě pak pro starší projekty jako Moodle.

(14) Zálohovaní serveru řídí prostředky operačního systému a systému záloh pomocí hypervisoru ve spolupráci se software Synology Active Bussiness Backup. Zálohy jsou ukládány na síťový server NAS

umístěný odděleně od serveru. Kapacita NAS je dostatečná pro zálohování současného objemu dat a realizaci pokročilé ochrany záloh před kompromitací např. snapshoty či obdobnou technologií.

(15) Škola disponuje centrální databází uživatelských identit Active Directory a využívá ji pro ověřování identity všech uživatelů přistupujících k síťových prostředků.

(16) Přístup do počítačů (resp. operačních systémů) je řízen převážně ověřováním vůči doméně Active Directory. Pouze malá část (méně než 10%) využívá ověřování lokálními uživatelskými účty.

(17) Hlavní softwarovou platformou serverů i uživatelských počítačů jsou operační systémy společnosti Microsoft a OpenSuse. Na koncových počítačích učitelů i žáků jsou používány převážně operační systémy Windows 10 a vyšší s podpory domény Active Directory. Škola provozuje aktuálně téměř 190 zařízení. Správa životního cyklu operačních systémů a aplikačního vybavení se provádí manuálně. Ochrana počítačů před škodlivým software je zajišťována systémem ESET Internet Security.

(18) Škola využívá a prostřednictvím internetu vzdáleně zpřístupňuje webové aplikace – internet školy (https://www. Goaml.cz), školský informační systém Bakaláři (https://bakalari.goaml.cz/). Aplikace jsou publikovány na IPv4 adresách, jsou dostupné šifrovaným protokolem https zabezpečeným certifikáty vydanými veřejnými certifikačními autoritami.

(19) Škola využívá aktuálně 18 tabletů, 4 síťové tiskárny a 170 počítačů pevných počítačů a notebooků. Plánovaný cílový počet během následujících 5 let může dosáhnou počtu 250. Průměrné stáří stávajících počítačů přesahuje 5 let. Počítače jsou vybaveny systémem Windows verze 10 a 11 ve verzi podporující doménu Active Directory.

(20) Od 1.11.2024 škola nově využívá: Licence Microsoft v programu EES CZESHA pro školy

M365 A3 Unified Edu Sub Per User	**39 licencí**
Win Server Standard Core ALng LSA 16L	**2 licencí**
M365 A3 Unified Edu Sub Student Use Benefit Per User	**780 licencí**

3 Popis cílového stavu a specifikace předmětu plnění

Základní požadavky na technické řešení

(1) V rámci projektu bude maximalizováno využití technických a systémových prostředků pořízených v předchozích projektech nebo vlastní investicí formou sdílení těchto prostředků tam, kde je to technicky, provozně a z pohledu bezpečnosti vhodné a možné.

(2) Cílem projektu je zvýšení bezpečnosti a související modernizace IT infrastruktury, aby implementací projektu byly naplněny Standardy konektivity škol[1] (dále jen Standard konektivity) a rozšířena funkčnosti ICT prostředí zapojených škol. Dílčí cíle dle jednotlivých komodit jsou specifikovány následovně:

Označení	Komodita
A	Rozvody LAN
B	Zabezpečení LAN a Wifi
C	Centrální logování
D	Server, zálohování a licence operačních systémů
E	Koncová zařízení

(3) Je požadováno řešení zachovávající a rozvíjející současné softwarové platformy Microsoft pro zachování kompatibility se stávajícími systémy a aplikacemi. Přechod na jinou platformu by způsobil zásadní uživatelské a provozní potíže.

(4) Je požadována unifikace jednotlivých komodit (tj. jejich realizace stejnými prostředky) pro všechny části z důvodu jednotné správy celého prostředí a odpovídající minimalizace provozních nákladů.

(5) Pokud prodávající (dále jen jako „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.

(6) 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 ceny za pořízení a provoz v rámci příslušných částí stanovené v Zadávací dokumentaci.

(7) Kupující (dále též jako „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.

(8) Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky:

- jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
- mají plnou záruku od výrobce,
- mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
- obsahují všechny nezbytné licence na používání příslušného softwaru,
- jsou v databázi výrobce uvedeny jako prodaná kupujícímu,
- jsou určeny pro provoz v České republice.

[1] Viz. aktuální verze https://www.edu.cz/digitalizujeme/standard-konektivity-skol/

(9) 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.

(10) Veškerá realizační dokumentace dodávaná v rámci 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.

4 Specifikace dodávaných technologií

Zadavatel požaduje, aby nabízená řešení měla požadované funkce již v době podání nabídky, nikoliv aby se jednalo o budoucí funkce plánovaných verzí software pro nabízené řešení.

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

Označení jednotlivých částí koresponduje s členěním ve Výkazu výměr.

Komodita A - Rozvody LAN		
Část	**Parametr**	**Popis povinného parametru**
Kabelové rozvody včetně příslušenství	Popis	Kabelové rozvody včetně příslušenství a souvisejících služeb dle podrobného výkazu výměr
	Záruka	Kabelové rozvody 10 let, rozvaděče 24 měsíců

Komodita B - Zabezpečení LAN a Wifi		
Část	**Parametr**	**Popis povinného parametru**
B001 **Perimetrový firewall 1ks**	Provedení	Umístitelné do racku
	HW parametry	Počet síťových rozhraní LAN RJ45 1 Gb - min 14x nebo jiná technicky kvalitnější kombinace portů (např. 2x 10Gb a 6x 1Gb)
		Počet rozhraní USB pro připojení ext. modemu - min. 1x
	Výkon	Propustnost firewallu min. 20 Gb/s nezávisle na velikosti paketu
		Propustnost firewallu - min. 15 Mpps (pps - paketů za sekundu)
		Počet FW politik min. 10 000
		Počet současných otevřených spojení - min 1,5 M
		Propustnost VPN - min. 11,5 Gbps
		Propustnost IPS - min 2,6 Gbps
		Propustnost antiviru - min. 1 Gbps
	Funkce	Režim vysoké dostupnosti - Active Active, Active Passive, Clustering
		Režim fungování L2 – transparentní režim, L3 – NAT/Router
		Podpora multicast, vytváření politiky pro multicast routování
		Podpora VPN: IPSec, SSL (portálový režim, tunelový režim), IPSEC (IKE, manual key, certifikát, gateway to gateway, hub and spoke, dial up konfiugrace, internet browsing konfigurace, podpora vice tunelů – redundantní VPN
		Podpora IPv6
		Podpora virtualizace (min. 10 virtuálních kontextů - firewallů)
		Podpora dynamických routovací protokolů - OSPF, PPTP, L2TP, GRE
	Firewall	Možnost nastavovat firewall politiku na základě geografických údajů.
		Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru Active Directory.
		Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offload.
		Podpora centrální NATovací tabulky
	Filtrační funkce	Možnost výběru mezi file based režimem (buffer) nebo flow based (inspekce on-the-fly)
		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)
		Email filter – antispamová a antivirová inspekce elektronické pošty

Komodita B - Zabezpečení LAN a Wifi		
		Intrusion Protection System – detekce útoků založena na signaturové části a na anomálním filtru, možnost vytvářet vlastní signatury.
		Web Filter – 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.
		Application Control – detekce, monitoring, povolení či zakázání vice než 2000 síťových aplikací na základě signatury dané aplikace, nikoliv dle portu.
		Kontrola komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S)
		DoS Policy prevence proti základním útokům typu DoS, syn proxy
	Ověřování uživatelů	LDAP, Active Directory, Radius, TACACS+, Ověřování na základě certifikátu
		Podpora silné autentizace uživatelů – integrovaná podpora generátoru jednorázových hesel (OTP) – Token pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů
		Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření.
	Dynamické routování	RIP, BGP, OSPF, IS-IS
		Policy routing
		Traffic Shaping, QoS s podporou DSCP markování a ToS
		Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu
		WAN optimalizace (optimalizace vybraných protokolů, byte chaching), Web Cache, Explicitní Proxy, Reverzní prózy, WCCP
	Reporty	Integrované logování a reporting, možnost vytváření vlastních reportů
	SFP+ moduly a patch cordy	Součástí dodávky jsou potřebné originální SFP+ moduly a optické/metalické propojovací kabely pro realizace díla.
	Záruka	Záruka výrobce min. 60 měsíců v režimu 24x7 na HW, OS, firmware a kompletní bezpečnostní SW. SW musí obsahovat IPS, AV, Web Filtering a Antispam aktualizace.
B002 **Centrální přepínač školy 1x**	Základní parametry	L2/L2+ přepínač v rackovém provedení max. 1U
	Porty	Min. 16x 10 Gb SFP+, vyhrazený samostatný LAN port pro management
	Propustnost	propustnost min. 300 Gbps
	Agregace portů	podpora LACP
	Správa	správa prostřednictvím kontroléru s plnou integrací (tj. kompletní správa prostřednictvím kontroléru a vyčítaní všech statusů do něj, vzdálený upgrade firmwaru z kontroléru)
	Podpora protokolů	podpora IPv6, Storm control, Spanning tree protocol
	VLAN	podpora VLAN, min. 500 aktivních VLAN současně (VLAN Group)
	Ověřování uživatelů a zařízení	podpora 802.1X
	MAC	podpora min. 20 000 MAC adres pro použití jako centrální switch (router)
	Routing	podpora statického routingu, min. 16 IPv4/IPv6 interface
	Port management	Rozšířený port management: VLAN, 802.1X autorizace, Radius VLAN, mirroring, agregace portů, pojmenování portů
	Napájení	interní redundantní zdroje (min 2)
	Monitoring a správa	plná podpora CLI, SSH, SNMP, syslog, sFlow, web rozhraní
	Záruka	min. 60 měsíců poskytovaná výrobce zařízení, a to včetně nároku na nové verze firmware
	Společné parametry	
B003 **Přístupové přepínače 8 ks**	Základní parametry	L2+ přepínač v rackovém provedení max. 1U
	Porty	min. 24x 10/100/1000Base-T RJ-45 porty + min. 4x 10 Gb/s SFP+ porty
	Propustnost	přepínací kapacita min. 120 Gb/s
	Podpora protokolů	podpora IPv6, Storm control, Spanning tree protocol
	Správa	správa prostřednictvím kontroléru s plnou integrací (tj. kompletní správa prostřednictvím kontroléru a vyčítaní všech statusů do něj, vzdálený upgrade firmwaru z kontroléru)
	Port management	rozšířený port management: VLAN, 802.1X autorizace, Radius VLAN, mirroring, agregace portů, pojmenování portů
	VLAN	podpora VLAN, min. 500 aktivních VLAN současně (VLAN Group)
	Ověřování uživatelů a zařízení	plná podpora 802.1X
	Záruka	min. 60 měsíců poskytovaná výrobce zařízení, včetně nároku na nové verze firmware
	Specifické parametry	

Komodita B - Zabezpečení LAN a Wifi		
B004 Přístupové přepínače s PoE 5 ks	Základní parametry	L2+ přepínač v rackovém provedení max. 1U
	Porty	min. 24x 10/100/1000Base-T RJ-45 porty + min. 4x 10 Gb/s SFP+ porty
	PoE	Všechny RJ-45 porty s podporou PoE+ napájení dle 802.3at, celkový PoE výkon min. 380W
	Propustnost	přepínací kapacita min. 120 Gb/s
	Podpora protokolů	podpora IPv6, Storm control, Spanning tree protocol
	Správa	správa prostřednictvím kontroléru s plnou integrací (tj. kompletní správa prostřednictvím kontroléru a vyčítaní všech statusů do něj, vzdálený upgrade firmwaru z kontroléru)
	Port management	rozšířený port management: VLAN, 802.1X autorizace, Radius VLAN, mirroring, agregace portů, pojmenování portů
	VLAN	podpora VLAN, min. 500 aktivních VLAN současně (VLAN Group)
	Ověřování uživatelů a zařízení	plná podpora 802.1X
	Záruka	min. 60 měsíců poskytovaná výrobce zařízení, včetně nároku na nové verze firmware
	Specifické parametry	
B005 Kontrolér 1 ks	Základní funkce	Kontrolér je určený pro řízení a správu switchů a WiFi přístupových bodů. Může být dodán jako samostatné HW zařízení nebo virtuální nebo softwarové řešení
	Počet spravovaných zařízení	min. 80 access pointů a 20 switchů
	Licence	trvalá, žádné licenční poplatky
	LAN porty	min. 1x port 10/100/1000Base-T RJ45 pro připojení do sítě
	Rozhraní	uživatelsky příjemné grafické rozhraní, web rozhraní
	Možnosti konfigurace	hromadná (dávková) konfigurace
	Informace o provozu	statistiky provozu, online zobrazování událostí a upozornění
	Přístupy pro hosty	generovaní voucherů pro přístup – 1, 4, 8hodin, 1, 7dní s možností tisku na běžné kancelářské tiskárně – Hotspot, Guest portal
	Autorizace uživatelů	autorizace uživatelů ze serveru Microsoft Active Directory
	Upgrade	upgrade firmware v zařízeních
	Sledování provozu	vytváření mapy sítě (umístění zařízení a jejich status – online)
	Zálohování	zálohovaní konfigurace v online provozu
	Běh na L3 sítí	běh na L3 sítí (tj. spravované prvky se nemusejí nacházet jen v dané broadcast doméně)
	Politiky pro skupiny uživatelů	ACL a Group Policy pro provozní údaje pro dané skupiny uživatelů – šířka přenosového pásma, časové rozlišení provozu, systém autorizace
	Provedení	instalace do 19“ rozvaděče
	Záruka	min. 60 měsíců poskytovaná výrobce zařízení, a to včetně nároku na nové verze firmware
	Specifické parametry	
B006 WiFi přístupové body vnitřní (AP) 53 ks	Základní funkce	Přístupový bod (AP) standardu Wi-Fi 6 včetně montážního materiálu na stěnu nebo strop
	Frekvence	podpora WiFi 6 protokolu 802.11ax v obou pásmech 2,4 GHz a 5 GHz
	Anténní systém	min. 4 integrovaných antény (2 antény min. 3dBi pro 2,4GHz a 2 antény min. 5dBi pro 5GHz)
	Přenosové rychlosti	přenosová rychlost min. 574 Mb/s v pásmu 2,4 GHz a 2400 Mb/s nebo vyšší v pásmu 5 GHz
	Standardy	podpora 802.3at, 802.11n, 802.11ax, 802.1x včetně přiřazování do VLAN, podpora WiFi kanálu s šířkou 160 MHz
	Výstupní výkon	výstupní výkon min. 20 dBm v pásmu 2,4 GHz a min. (20-23 dBm – 100 až 200 mW), pokud bude pokrytí WiFi signálem v pásmu 5 GHz dostatečné pro spolehlivou práci všech připojených klientů
	Ladění kanálů	automatické ladění Wi-Fi kanálů a možnost detekce s reakcí na non-wifi rušení
	Multi SSID	podpora vysílání min. 6 SSID (WiFi sítí) v každém pásmu současně, podpora přiřazení každého SSID samostatné VLAN
	Provedení	provedení umožňující montáž na strop i stěnu, včetně držáku pro montáž
	Porty	min. 1x Gigabit Ethernet RJ-45 port pro připojení do sítě, s podporou aktivního PoE napájení dle normy 802.3af nebo 802.3at
	Šifrování	podpora WPA3 Personal/Enterprise šifrování
	Bezpečnost	autorizace uživatelů pomocí 802.1X
	Konfigurace	plná konfigurace z kontroléru
	Indikace	indikace provozního stavu pomocí LED
	Upgrade firmware	vzdálený upgrade firmware z kontroléru

Komodita B - Zabezpečení LAN a Wifi		
	Správa frekvenčního pásma	přechod klientů (roaming) mezi AP, automatické rozkládání zátěže mezi AP
	Záruka	min. 60 měsíců poskytovaná výrobce zařízení, včetně nároku na nové verze firmware
B007 WiFi přístupový bod venkovní (AP) 1 ks	Základní funkce	Přístupový bod (AP) standardu Wi-Fi 6 určený pro venkovní provoz, včetně montážního materiálu na sloup
	Frekvence	podpora WiFi 6 protokolu 802.11ax v obou pásmech 2,4 GHz a 5 GHz
	Anténí systém	min. 4 integrovaných antény (2 antény min. 3dBi pro 2,4GHz a 2 antény min. 5dBi pro 5GHz)
	Přenosové rychlosti	přenosová rychlost min. 574 Mb/s v pásmu 2,4 GHz a 1201 Mb/s v pásmu 5 GHz
	Standardy	podpora 802.3at, 802.11n, 802.11ax, 802.1x včetně přiřazování do VLAN
	Výstupní výkon	výstupní výkon min. 20 dBm v pásmu 2,4 GHz a min. 26 dBm v pásmu 5 GHz s možností regulace
	Ladění kanálů	automatické ladění Wi-Fi kanálů a možnost detekce s reakcí na non-wifi rušení
	Multi SSID	podpora vysílání min. 6 SSID (WiFi sítí) v každém pásmu současně, podpora přiřazení každého SSID samostatné VLAN
	Provedení	provedení umožňující montáž na stožár nebo na stěnu, včetně držáku pro montáž
	Porty	min. 1x Gigabit Ethernet RJ-45 port pro připojení do sítě, s podporou aktivního PoE napájení dle normy 802.3af nebo 802.3at
	Šifrování	podpora WPA3 Personal/Enterprise šifrování
	Bezpečnost	autorizace uživatelů pomocí 802.1X
	Konfigurace	plná konfigurace z kontroléru
	Indikace	indikace provozního stavu pomocí LED
	Upgrade firmware	vzdálený upgrade firmware z kontroléru
	Správa frekvenčního pásma	přechod klientů (roaming) mezi AP, automatické rozkládání zátěže mezi AP
	Odolnost	odolnost proti vlivu počasí (možnost použít AP přímo ve venkovním prostředí, tj. odolnost proti vodě, dešti, prachu, větru apod.)
	Provozní teploty	Nejméně v rozsahu -30°C až +60°C
	Záruka	min. 60 měsíců poskytovaná výrobce zařízení, včetně nároku na nové verze firmware
	Specifické parametry	
B008 Optické prvky	SFP+ modul	16 ks modulu SFP+ 10 Gb, SM, BiDi, 10 km – kompatibilní s nabízenými přepínači, LC konektor
	SFP modul	2 ks SFP modul, SM, kompatibilní s nabízenými přepínači, LC konektor
	DAC kabely	9 ks DAC kabelů pro SFP+ rozhraní, 2m, kompatibilní s dodanými aktivními prvky
	Optické patch kabely	18 ks kabel SM s konektory LC-SC, délka 3 m pro připojení přepínačů do optických tras
	Záruka	36 měsíců
B009 Systém 802.1X Eduroam	Popis	Instalace a konfigurace systému 802.1X pro zajištění autentizace uživatelů připojených přes LAN a WiFi prostředky do počítačové sítě školy. Systém je založený na protokolu RADIUS a je integrovaný s Active Directory. Připojení do federovaného systému Eduroam.
B010 Přepínač 1 ks	Základní parametry	L2+ přepínač v rackovém provedení max. 1U
	Porty	min. 8x 10/100/1000Base-T RJ-45 porty + min. 2x 1 Gb/s SFP porty
	Propustnost	přepínací kapacita min. 20 Gb/s
	Podpora protokolů	podpora IPv6, Storm control, Spanning tree protocol
	Správa	správa prostřednictvím kontroléru s plnou integrací (tj. kompletní správa prostřednictvím kontroléru a vyčítaní všech statusů do něj, vzdálený upgrade firmwaru z kontroléru)
	Port management	podpora VLAN, min. 500 aktivních VLAN současně (VLAN Group)
	Ověřování uživatelů a zařízení	plná podpora 802.1X
	Záruka	min. 60 měsíců poskytovaná výrobce zařízení, včetně nároku na nové verze firmware

Komodita C - Centrální logování, monitoring síťového provozu		
Část	**Parametr**	**Popis povinného parametru**
C001 Systém pro sběr a správu logů a	Požadavky na systém pro centralizovanou správu logů, událostí a strojových dat	Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware.
		Veškerá konfigurace systému se musí provádět v grafickém rozhraní jednotné uživatelské webové konzole. Systém poskytuje podporu pro vizuální programování pro všechny kroky zpracování strojových dat. Ve webové konzoli se nepřipouští konfigurace za využití skriptů, maker nebo textových konfiguračních polí, do kterých se složité textové skripty/makra vkládají.

Komodita C - Centrální logování, monitoring síťového provozu		
monitoring síťového provozu 1x		Systém umožňuje dopsání parserů pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému - Uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na vytváření zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů v jednotném ovládacím grafickém webovém rozhraní viz bod č. 1. Vytváření a testování parserů nesmí mít vliv na provoz systému. Pro psaní parserů nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Požadujeme předložit příslušnou dokumentaci k vytváření parserů a testování jejich funkčnosti.
		Systém umožňuje v grafickém rozhraní vizuálního programovacího jazyka snadno provádět třídění a značkování vstupních dat pro jejich další zpracování. Nepřipouští se nastavování třídění vstupních dat ve formě skriptu/makra zobrazeného v textovém okně. Předložte příslušný odkaz na dokumentaci popisující funkčnost třídění vstupních dat.
		Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém musí umožňovat příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále požadujeme podporu sběru strojových dat z databází s nastavením v grafickém menu systému minimálně pro databáze MSSQL, MySQL, Oracle a PostgreSQL a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta. Předložte detailní komunikační matrici s popisem všech použitých protokolů a portů pro nabízený systém a dokumentaci k nastavení sběru z databází v grafickém rozhraní systému.
		Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv. Integrované parsery systému automaticky přidávají ke zprávám, kterých se to týká, meta informace o jaký druh zprávy se jedná, minimálně požadujeme rozlišení těchto druhů zpráv: úspěšné přihlášení, neúspěšné přihlášení, odhlášení, konfigurační změna, značka/tag. Tyto meta informace musí být možné přidávat i v uživatelsky definovaných parserech.
		Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv. Integrované parsery systému automaticky přidávají ke zprávám, kterých se to týká, meta informace o jaký druh zprávy se jedná, minimálně požadujeme rozlišení těchto druhů zpráv: úspěšné přihlášení, neúspěšné přihlášení, odhlášení, konfigurační změna, značka/tag. Tyto meta informace musí být možné přidávat i v uživatelsky definovaných parserech.
		Hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a standardizovat alespoň na tyto základní druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými čísly je pak možné při prohledávání dat provádět matematické operace (součty všech hodnot, průměry, nejmenší/největší hodnota apod.).
		Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, které vzniká v okamžiku přijetí logu systémem a kterým se systém defaultně řídí.
		Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.
		Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.
		Systém nesmí v žádném případě umožnit mazání nebo modifikování již uložených logů v rámci požadované retence. A to ani libovolnou konfigurační změnou - administrátorovi s nejvyššími oprávněními k navrhovanému systému. Každý zpracovaný log musí mít dohledatelný unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.
		Systém musí umožňovat konfiguraci filtrace nerelevantních událostí v grafickém rozhraní vizuálního programovacího jazyka. Pro psaní filtrace nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Předložte odkaz na dokumentaci popisující způsob filtrování nerelevantních událostí.
		Systém provádí konsolidaci logů na interním storage logovacího systému.
		Systém umožňuje snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj musí být integrální součástí navrhovaného systému a musí se obsluhovat v jednotném rozhraní nabízeného produktu. Předložte link nebo pdf popisující způsob vytváření reportů.
		Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky.
		Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele.
		Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele.

Komodita C - Centrální logování, monitoring síťového provozu		
		Systém podporuje nativní získávání logů z Office365/Microsoft365 prostředí bez ohledu na použitou licenci 365 prostředí a bez nutnosti instalovat dodatečné externí komponenty. Požadujeme předložit link na dokumentaci popisující nastavení systému v jednotném grafickém rozhraní tak, aby získával logy z Office365/Mircosoft365.
		V případě krátkodobého (do 10 minut) až dvojnásobného přetížení systému proti jeho tabulkovým hodnotám nesmí dojít ke ztrátě logů nebo nesprávnému stanovení časového razítka. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti.
		Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno, zdrojová IP, značka/tag apod.).
		Dodavatel musí předložit potvrzení vystavené autorizovanou osobou o shodě, že nabízený systém splňuje požadavky normy ČSN/ISO 27001:2013 na pořizování auditních záznamů. Toto potvrzení není možné nahradit certifikátem na společnost dodavatele (subdodavatele) nebo výrobce nabízeného systému. Nelze nahradit čestným prohlášením.
		Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Továrně dodané pohledy na data nesmí jít administrátorem ani uživatelem systému nevratně modifikovat nebo smazat.
		Systém obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Pro vytváření nových pohledů na data není přípustné používat povinně SQL jazyk.
		Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.
		Na základě pohledu na uložená data lze provést export dat ve strukturovaném formátu tak, jak jsou v továrně nastaveném nebo uživatelsky nastaveném pohledu data skutečně zobrazena.
		Konfigurační a Systémové rozhraní a dokumentace k těmto rozhraním musí být identické v anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce nebo zjednodušená dokumentace odkazující na další dokumentaci v anglickém jazyce, případně na dokumentaci třetích stran. Požadujeme předložit link na online dokumentaci nebo připojit pdf aktuální kompletní dokumentace k ověření jednotlivých vlastností navrhovaného systému.
		Systém nabízí kapacitní i výkonovou škálovatelnost.
		Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 4TB.
		Požadujeme, aby systém obsahoval REST-API pro integraci s externím monitorovacím systémem (Zabbix, Nagios, MRTG a další) a umožňoval autorizovaný přístup ke strukturované databázi logů. Požadujeme předložit vzorový návod na integraci s externím monitorovacím systémem.
		Dodavatel doloží prohlášení výrobce o shodě s požadavky Vyhlášky 82 / 2018 Sb. „o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)" k Zákonu 181 / 2014 Sb. „o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)".
		Jednotná centrální webová konzole s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. Není přípustné, aby navrhovaný systém měl více rozdílných konzolí od různých výrobců s rozdílným ovládáním nebo aby se konfigurace musela provádět mimo jednotné webové rozhraní. Požadujeme předložit dokumentaci, ze které je zřejmé, jakým způsobem je realizována konfigurace v rámci jednotné konzole.
		Požadujeme, aby systém umožňoval jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem na základě typu zdrojů a značek a k jednotlivým ovládacím komponentům systému. Připojte odkaz na dokumentaci popisující vytváření uživatelských rolí v grafickém rozhraní systému.
		Dodaný systém musí obsahovat ucelené all-in-one řešení pro parsování a normalizaci přijatých událostí bez nutnosti dodatečné instalace externích aplikací nebo systémů. Jedinou přípustnou výjimkou je monitorování systémů Windows pomocí agentů.
		Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem.
	Kompatibilita	VMWare ESXi a Microsoft Hyper-V
	Podpora	Minimálně 60 měsíců včetně poskytnutí nových a opravných verzí

Komodita D – Server, diskové pole, UPS a zálohování		
Část	**Parametr**	**Popis povinného parametru**
D001	Provedení	RACK 19", včetně výsuvných kolejnic, celková výška maximálně 2U, zaručený provoz při teplotě 30°C
	Procesor	2 sockety, osazen jeden CPU, každý právě 16 jader, min. základní frekvence 2,0 GHz, min. frekvence MEMBUS 4400 MHz, max. TDP 150W.

Server 1x		Požadovaný výkon při osazení 2x CPU min.: - SPECrate2017_int_base min. 282 - SPECrate2017_fp_base min. 368 - Overall SPECpower_ssj2008 min. 14000 Požadujeme CPU poslední generace.
	Paměť	RAM min. 128 GB, 32 paměťových slotů, min. rozšiřitelnost až na 8 TB, osazeno 4x 32GB 2Rx8 DDR5-4800 Reg ECC
	Pevné disky	Min. 1x 240 GB SSD. Disk musí být hot-plug, server obsahuje dalších min. 7 volných funkčních 3,5" slotů pro disky.
	Porty	Min. 5x USB port v3.0 nebo vyšší: - min.2x přední - min 2x zadní, - min. 1x interní. Možnost osadit sériový port nezabírající PCIe slot.
	Chlazení	Redundantní hotswapové ventilátory
	LAN	min. jeden 1 Gbit RJ45 port nezabírající PCIe slot 4x 10 Gbps SFP+ 4x 1 Gpps TP
	PCI sloty	Volné PCIe sloty: - min. 1x PCI-Express 5.0 x8 a - min. 3x PCI-Express 5.0 x16
	Vzdálená správa	HW management, zapnutí, vypnutí, restart serveru, přesměrování KVM nezávislé na OS, vzdálené připojení médií. Interní management serveru umožňuje update serveru online z OS i offline bez nutnosti instalace dalšího nástroje pro správu, umožňuje bootu a instalace z interní SD karty o velikosti alespoň 16 GB. Dedikovaný LAN port pro management 1 Gbps RJ45. Možnost sdílení management portu s jiným Ethernet portem serveru. Časově neomezená licence.
	Napájení	2x redundantní napájecí zdroj min. 850 W každý, účinnost min. 96% Titanium, server musí běžet i při napájení pouze jednoho zdroje. Napájecí kabely min. 2,5 m. Spotřeba serveru v nabízené konfiguraci při 100% zatížení max. 360 W.
	Podpora operačních systémů a hypervizorů	Podpora nejrozšířenějších operačních systémů (Windows Server, Linux, VMware ESX) v nejnovější verzi
	Záruka	min. 60 měsíců poskytovaná **výrobcem v místě instalace** s reakcí nejpozději následující pracovní den po nahlášení závady
D002 **Diskové pole 1x**	Provedení	Diskové pole s výškou max. 2U, včetně montážního materiálu do racku (ližiny pro rack), maximální montážní hloubka 500 mm.
	Pozice, rozšiřitelnost	minimálně 24 pozice pro HDD/SSD formátu 2,5", rozšiřitelnost minimálně na 48 disků.
	Spotřeba	Maximální spotřeba celé konfigurace při 100% zatížení 480 VA.
	Propustnost, latence	Minimální propustnost kontrolérů pole 100000 IOPS.
	Podporované typy disků	Podporované typy disků a jejich libovolné kombinace 3.5" Nearline SAS 22TB/18TB/12TB/8TB/4TB (7,200 rpm), 2,5" SSD 15,3TB/7,6TB/3,8TB/1,9TB/1,6TB, 2.5" SAS 1,8TB/1,2TB (10,000 rpm), možnost použití disků SED nebo FIPS.
	Podpora RAID technologií	Podpora typů RAID 0, 1, 1+0, 3, 5, 6, DDP s funkcí rychlého zotavení. Trvalá licence pro všechny uvedené typy RAID.
	Osazení disky	Minimální osazení disky: 6 kusů SAS 1,8TB 2,5" 10kRPM a 6 kusů disků SSD 1,9TB.
	Využitelná kapacita	Min. čistá využitelná kapacita pro připojené servery 8,5TB SAS (s nastavenou ochranou proti výpadku jednoho disku, např. RAID5) a 6,9TB SSD (s nastavenou ochranou proti výpadku jednoho disku, např. RAID5).
	Řadiče	2 redundantní řadiče iSCSI, každý s 2x SFP+ rozhraním s rychlostí 10 Gbps
	Kabely	2x DAC aktivní kabel 10Gb 5m.
	Vyrovnávací paměť (cache)	Minimální kapacita cache 16GB.
	Ochrana cache	Ochrana cache řadičů vůči výpadku napájení. V případě výpadku napájení musí být neuložená data zachována.
	Front-End porty	Minimální počet konfigurovatelných Front-End portů 8 na celé pole. Podporované typy Front-End portů FC 16 Gbps LC, iSCSI 1 Gbps RJ45, iSCSI 10 Gbps SFP.

	Přístup k managementu	Management porty LAN port 10/100/1000 Mbps min. 1 na každém řadiči. Bezpečný přístup k managementu pomocí protokolů SSL a SSH.
	Počet iSCSI portů	Minimální počet konfigurovaných iSCSI portů 10 Gbps SFP+ 4 ks.
	Správa diskového pole	SW pro kompletní vzdálenou správu pole + webové rozhraní, které umožní kompletní správu pole z libovoln0ho webového prohlížeče.
	Počet snapshotů	Minimální počet snapshotů a klonů 128.
	Licenční politika	Žádná dodaná licence nesmí být vázána na počet připojených serverů ani na kapacitu diskového pole ani na jednotlivé disky a pokud ano, tak musí pokrývat celkovou maximální rozšiřitelnost pole.
	SNMP, hlášení poruch	Podporované verze SNMP v2c, REST. Podpora zasílání alertů e-mail alert a trap, integrovatelné do nástrojů pro vzdálenou správu, požadujeme aktuální MIB soubor po každé aktualizaci fw.
	HOT-PLUG technplogie	Všechny komponenty pole musí být hot-plug, zejména řadiče, ventilátory, zdroje, IO moduly a pevné disky.
	Minimální počet připojených serverů	Minimální počet připojitelných serverů 128. Licence pro jejich připojení a MPIO musí být součástí nabídky.
	Provozní parametry	Rozsah provozních teplot 5-40°C, rozsah provozních vlhkostí 10-85%.
	Záruka	min. 60 měsíců poskytovaná **výrobcem v místě instalace** s garantovanou reakcí nejpozději následující pracovní den po nahlášení závady.
D003 **UPS pro server** **1 ks**	Provedení	UPS min. 2200VA, provedení do Racku, výška max. 2U, max. hloubka 70 cm
	Výstupní výkon	min. 1950W
	Doba provozu na baterie	Min. 45 minut při zátěži 400W, min. 28 min. při zátěži 600W
	Topologie	Line-interactive
	Výstupní přípojky	min. 8ks typu IEC 320 C13 (všechny umožňují provoz na baterie)
	Vstup	Jmenovité vstupní napětí [V]: 230 Kmitočet na vstupu [Hz]: 50/60 Hz +/- 3 Hz (autodetekce) Rozsah vstupního napětí pro napájení z rozvodné sítě: 160 – 286V
	Komunikace a správa	Port rozhraní: RJ-45 10/100 Base-T, RJ-45 Serial, SmartSlot, USB Ovládací panel: LED diody zobrazují stav – minimálně: - napájení ze sítě - napájení z baterie - vyměnit baterii - přetížení Zvukové upozornění: Upozornění na stav, kdy je systém napájen z baterie, zřetelné upozornění na nízkou kapacitu baterie
	Příslušenství	Hardware pro montáž do stojanu, skříňové podpěrné lišty, signalizační kabel, teplotní čidlo, kabel USB
	Softwarová podpora	Součástí dodávky bude software pro běžné typy virtualizačních platforem (VMWARE, Microsoft Hyper-V), který umožní podle nastavených parametrů řádné ukončení práce virtuálních serverů a následné fyzické vypnutí serveru. Trvalá licence.
	Záruka	Minimálně 36 měsíců
D004 **Zálohovací zařízení** **1 ks**	Provedení	Samostatně stojící, možno umístit i mimo rack
	Pozice pro disky	Min. 8 pozic pro HDD / SSD, podpora Btrfs a ext4 souborových systémů, min. 1x PCIe Gen3 x2 slot pro rozšiřující kartu
	Operační paměť	Min. 8 GB DDR4 RAM
	Rozšiřitelnost	Podpora připojení externích disků přes USB 3.0 (min. 2 porty) + min. 1x eSATA port 2 x M.2 NVMe 2280 SSD slot pro SSD cache
	Výkon	Přenosová rychlost až 2300MB/s při osazení 10Gb LAN, IOPS při náhodném čtení 4K až 110 000
	Komunikace LAN	Síťové protokoly CIFS, WebDAV, iSCSI, SSH, SNMP, http/s
	Hot-swap	Disky vyměnitelné za chodu
	Kapacita	Osazeno min. 6ks 12TB HDD SATAIII/7200 RPM/256MB cache. Disky se zárukou 60 měsíců, uvedené v seznamu kompatibilních disků výrobce zálohovacího zařízení, automatická aktualizace firmware společně s aktualizacemi operačního systému zálohovacího zařízení.
	Konektivita	Min. 4x 1GBit Ethernet porty s podporou agregace linek a redundance. Min. 2x 10Gbit SFP+ porty
	Disková cache	Osazeny 2 ks SSD M.2 NVMe modulů s kapacitou min. 400 GB (cache pro čtení i zápis)

	Ochrana dat	Basic/JBOD/0/1/5/5+Spare/6/10 + Hybrid RAID
	Podpora	Podpora virtualizace a iSCSI (VMware vSphere® 6,5, Microsoft Hyper-V®, Citrix®, OpenStack®), podpora Windows ADS, podpora AES 256bit šifrování svazku
	Software	Zařízení musí obsahovat časově neomezené služby pro zálohování pracovních stanic, pro zálohování jiných zařízení NAS, pro zálohování fyzických i virtuálních serverů a pro zálohování Microsoft 365 a G-Suite.
	Podpora UPS	Podpora korektního vypnutí signálem z UPS přes LAN při výpadku napájení
	Záruka	Minimálně 36 měsíců
D005 **UPS pro zálohovací zařízení** **1 ks**	Provedení	Volně stojící
	Příkon	Min. 1200VA
	Výkon	Min. 650W
	Zásuvky	České zásuvky, minimálně 4 ks
	Komunikace	USB port
	Záruka	Min. 24 měsíců
SW pro virtualizaci	Využití licence zadavatele	Pro instalaci virtuálních serverů bude použit hypervizor VMWARE vSphere 8 Essentials kit - zadavatel má zakoupenou trvalou licenci s podporou do 31. ledna 2027.
D006 **SW licence zálohovací software** **1ks**	Licence	Licence zálohovacího software pro min. 10 zálohovaných zařízení (nerozlišuje se mezi VM, fyzickýcm serverem, PC - univerzální použití licence) bez omezení objemu dat
	Efektivita ukládání dat	Integrovaná technologie komprimace a deduplikace.
	Nároky na správu	„Bezagentové" řešení – není nutná instalace agentů do zálohovaných virtuálních serverů nebo aplikací. Možnost replikace virtuálních strojů na jiný virtualizační nod za chodu serveru
	Ochrana dat	Provádění datově konzistentních záloh hlavních serverových aplikací - MS SQL, Active Directory, souborové systémy - bez nutnosti odstávky aplikace
	Fyzické servery	Vestavěná podpora zálohování fyzických serverů - pro fyzické servery je přípustné využívat agenty. Podpora ukládání záloh nevirtualizovaných serverů a PC do společného úložiště a monitorování zálohovacích úloh.
	Snapshoty	Využívání snapshotů, zálohování pouze dat změněných od poslední úspěšné zálohy. Podpora operačních systémů Windows a Linux v zálohovaných virtuálních serverech.
	Ověření záloh	Možnost otestování a ověření každého zálohovaného VM a jeho obnovitelnosti spuštěním přímo ze souboru zálohy; včetně podpory pro vlastní testovací skripty.
	Obnova položek Active Directory	Obnova jednotlivých objektů i skupin objektů Active Directory – uživatelů, skupin, kontejnerů, objektů Group Policy včetně hromadného výběru a obnovy hesel účtů
	Uložiště záloh	Možnost ukládání záloh na diskový prostor. Možnost nouzového spuštění zazálohovaného virtuálního serveru z NAS v izolovaném prostředí bez nutnosti obnovy
	Správa	Vytváření a správa úloh (zálohování, obnova apod.) pomocí průvodců. Automatický reporting úspěšných i neúspěšných úloh. Běžné úlohy obnovy (obnovení souboru, databáze SQL, objekty Active Directory) provádět pomocí průvodců.
	Záruka a nárok na nové verze	Záruka 60 měsíců včetně nároku na nové verze software.
D007 **Rack pro server**	Provedeni	Rack 42U pro umístění serveru, diskového pole a UPS, šířka 800 mm, hloubka 1200 mm, přední i zadní dveře perforované
	Police	2x Police 1U/750mm, s nosností až 80 kg
	Chlazení	Ventilátorová jednotka vrchní včetně termostatu

Komodita E – Koncová zařízení		
Část	**Parametr**	**Popis povinného parametru**
E001 **Notebook** **22 ks**	Displej	Úhlopříčka min. 16", poměr stran 16:10, rozlišení min. 1920 x 1200 bodů
	CPU	CPU s bodovým hodnocením min. 16 000 bodů dle https://www.cpubenchmark.net/
	RAM	Min. 16 GB
	Disk	Podpora PCIe® 4.0x4 NVMe®, osazený 1 ks SSD disk s kapacitou min. 500 GB + možnost doplnit další SSD s kapacitou až 2 TB
	Připojení	Bluetooth verze min. 5.1, WIFI standardu 6, Ethernet 10/100 Mbit/s
	Kamera	Kamera s FHD rozlišením a s krytkou

	Porty	1x Ethernet (RJ-45) 1x HDMI® 2.1, až 4K/60Hz 1x kombinovaný konektor pro sluchátka / mikrofon (3,5 mm) 1x čtečka SD karet 1x Thunderbolt™ 4 / USB4® 40 Gbps (podpora přenosu dat, Power Delivery 3.0 a DisplayPort™ 1.4) 1x USB 3.2 Gen 1 1x USB 3.2 Gen 1 (vždy zapnuto) 1x USB-C® 3.2 Gen 2 (podpora přenosu dat, Power Delivery 3.0 a DisplayPort™ 1.4)
	Klávesnice	Podsvícená klávesnice s CZ/SK popisy a s numerickou částí
	Zvuk	Stereo reproduktory, 2W x 2, Dolby® Audio™, 2x mikrofon
	Zabezpečení	Firmware TPM 2.0 , snímač otisků prstů, IR kamera pro Windows® Hello
	Baterie	Min. 45 Wh
	Napájecí adaptér	Min. 65W, napájení notebooku přes USB-C port
	Mechanická odolnost	Kovový horní kryt (například hliník)
	Certifikace	ENERGY STAR® 8.0, certifikace TCO 9.0, soulad s RoHS
	Certifikace odolnosti	Vojenský test MIL-STD-810H
	Operační systém	WINDOWS verze PRO v nejnovější dostupné verzi (nutné pro zajištění 100% kompatibility s provozovanými aplikacemi)
	Záruka	Min. 36 měsíců poskytovaná výrobcem s opravou v místě instalace (on-site)
E002 **Dokovací stanice pro notebook** **21 ks**	Popis	Dokovací stanice USB-C 100% kompatibilní s dodanými notebooky
	Video porty	Min. 2x DP, 1x HDMI
	USB porty	Min. 3x USB 3.1, 2x USB 2.0, 1x USB-C
	Audio porty	1x Combo 3,5 mm audio Jack
	Ethernet	Min. 1x Gigabit Ethernet
	Power Delivery	Min. 65W s 90W napájecím adaptérem (součást dodávky)
	Záruka	Min. 36 měsíců
E003 **Projektor včetně držáku a montáže** **17 ks**	Popis	Projektor do učeben s možností montáže na strop
	Rozlišení	1920x1080 bodů, poměr stran 16:9
	Svítivost [lm]	Min. 4000
	Kontrast	Min. 16000:1
	Životnost lampy [h]	Min. 6500 v běžném režimu, 17000 (v úsporném režimu
	Rozhraní – minimálně	- USB 2.0 Type A - USB 2.0 Type B - RS-232C - Wired Network - VGA in (2x) - VGA out - HDMI in (2x) - Composite in - Stereo mini jack audio out - Stereo mini jack audio in (2x) - Cinch audio out - Microphone input - Wireless LAN IEEE 802.11b/g/n - Miracast
	Další požadavky	Dodávka včetně stropního držáku a potřebných propojovacích kabelů

5 Požadavky na instalační a implementační práce

Součástí dodávky technologií bude jejich dodávka, instalace a implementace do prostředí kupujícího s jejich konfigurací v rozsahu tak, aby došlo k naplnění požadavků standardu konektivity uvedeného v tabulce níže. Veškeré možné související dodávky a služby, které plynou z tabulky uvedené níže prodávající musí zohlednit ve svém plnění a dodat tak, aby došlo k plnění požadovaných parametrů konektivity definovaných v této tabulce.
Součástí předmětu plnění jsou dále i služby a práce prodávajícího se zařízeními a licencemi přímo související a nezbytné k řádnému uvedení předmětu plnění do provozu:

- Provedení předimplementační analýzy (včetně plánovaných změn v konfiguraci současné infrastruktury) a zpracování detailního finálního popisu cílového stavu a postupu implementace.
- Zpracování prováděcí dokumentace, podle které bude dodavatel řešení implementovat. Prováděcí dokumentace musí být před zahájením implementace výslovně schválena zadavatelem. Prováděcí dokumentace musí vycházet z předimplementační analýzy a respektovat a využívat osvědčené praktiky (tzv. Best Practices) a doporučení výrobců nabízených technologií.
- Dodávka a implementace předmětu plnění dle schválené prováděcí dokumentace včetně technické podpory.
- Zajištění projektového vedení realizace předmětu plnění.
- 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
  - 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 10 a vyšších, Android, iOS a MacOS.
- Zpracování dokumentu Zásady využívání ICT a přístupu k síti dle Standardu konektivity pro začlenění do vnitřních předpisů školy.
- Zpracování materiálů pro školení a provedení školení.
- Zajištění zkušebního provozu infrastruktury v délce minimálně 2 týdnů včetně technické podpory specialistů na dané zařízení/službu s dostupností maximálně do 2 hodin na místě realizace od nahlášení požadavku v pracovní den v době od 8h do 17h.
- zpracování a předání instalační dokumentace,
- zpracování a předání administrátorské dokumentace
- Provedení akceptačních testů.
- Předání do plného provozu.

Požadujeme, aby práce mající dopad do fungování IT prostředí kupujícího, byly prováděny výhradně mimo dobu výuky (tedy byly prováděny v časech 16:00 – 6:00, případně mimo pracovní dny kdykoliv). Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standartních formátech (např. MS Office) používaných kupujícím na datovém nosiči a 1x kopii v papírové formě.

5.1 Instalační a implementační služby v oblasti sítě

Po dokončení plnění dle této specifikace bude škola plně pokryta LAN i WiFi sítěmi s parametry vyhovujícími technickým požadavkům Standardu konektivity. Školní síť bude podporovat IPV6, bude

chráněna Firewallem a provoz na síti bude monitorován a logován. Přístup do sítě bude zabezpečen protokolem 802.1X. Jedná se zejména o následující:

- Bude implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby s využitím technologie 802.1x.
- 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.
- 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).
- Architektura WiFi bude založena na řešení s centrální správou prováděnou hardwarovým, SW, nebo virtuálním kontrolérem (řadičem). Kontrolér 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.
- Ověřování přístupu do LAN bude realizováno protokolem 802.1x vůči adresářové službě prostřednictvím protokolů radius a P/EAP. Používaná zařízení (min. stolní i přenosné počítače) budou vybavena tzv. suplikantem-softwarovou komponentou, která dokáže předávat ověřovací požadavky síťovým prvkům, které tyto požadavky ověří vůči adresářové službě. 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.
- 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 radius servery. Učitelé a žáci budou prostřednictvím radius serveru ověřováni v adresářové služby. Zabezpečení vnitřních sítí (BSSID) školy bude provedeno dle 802.1i, tedy-WPA3 (v odůvodněných případech 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 nebo jiné technologie s tzv. lobby přístupem pro správu a generování účtů/kupónů ne-technickou osobou.
- Federovaný systém EDUROAM (www.eduroam.cz) umožňuje přistupovat k sítím subjektů zapojených v systému a prostřednictvím těchto sítí k dalším službám, typicky internetu. Federace umožňuje ověření uživatele v libovolné zapojené síti (v České republice i zahraničí) pomocí uživatelovy jediné (centrální) identity. Správcem systému EDU je společnost Cesnet. V rámci projektu bude realizováno připojení do systému EDUROAM a bude nakonfigurováno

připojení WiFi sítě do systému EDUROM prostřednictvím vybudované autentizační a autorizační platformy na bázi radius serverů a adresářové služby. Současně budou realizovány další netechnické požadavky pro provoz EDUROAM – zejména vytvoření informační webové stránky a zajištění technického kontaktu. Zapojení do systému EDUROAM umožní národní i mezinárodní mobilitu žáků a učitelů.

V rámci výše uvedeného nasazení technologií budou provedeny minimálně následující služby:

- Analýza stávajícího síťového prostředí a návrh nového architektury LAN i WiFi
- Implementace pořízených technologií
- Provedení segmentace LAN – VLAN, adresování, směrování/routování
- Zavedení IPv6 pro přístup k internetovým zdrojům publikovaným na IPv6 adresách
- Zavedení IPv6 pro veškeré publikované služby z interních či externích prostředků. Včetně součinnosti pro zajištění změn u externích poskytovatelů služeb. Jde zejména (ale ne výhradně) o služby hostování domén škol, DNS, e-mail, weby škol, publikované nebo hostované školské informační systémy.
- Zavedení DNSSEC pro interní DNS služby i součinnost při zabezpečení domén škol. Dodavatel poskytne škole písemně parametry nutné pro správnou konfiguraci DNSSEC u poskytovatele internetového připojení. Škola zajistí nutnou součinnost pro správné nastavení parametrů DNSSEC.
- 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
- Návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) pro školy
- Vybudování VPN pro vzdálený přístup uživatelů LAN na bázi webového portálu s využitím dodaných technologií.
- Návrh a provedení akceptačních testů, musí zahrnovat testy propustnosti LAN a pokrytí WiFi

5.2 Instalační a implementační služby v oblasti centrálního logování

Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací. 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).
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.
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.
Z pohledu požadavku 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. 3 měsíce. Na tento rozsah retence musí být systém dostatečně

dimenzován, tak aby nedocházelo k výkonovým problémům a systém měl dostatečnou rezervu pro očekávatelný budoucí nárůst informací a jejich zdrojů.
Technicky se může jednat o virtuální appliance nebo o samostatné komplexní řešení. V případě, že bude použito virtuální řešení nainstalované na centrálním serveru, nesmí systém centrálního logování při plné zátěži spotřebovat více než 30% systémových zdrojů centrálního serveru.
V rámci výše uvedeného nasazení technologií budou provedeny minimálně následující služby:

- 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.)
- Provedení souvisejících konfigurací monitorovaných systémů (vyplývá z požadavků standardu konektivity)
- Návrh a provedení akceptačních testů, musí zahrnovat ověření logování veškerých požadovaných uživatelů a správnost přiřazení identit uživatelů logovaným údajům

5.3 Instalační a implementační služby v oblasti serveru, zálohování data a energie a serverových operačních systémů

V rámci plnění bude nasazen nový server, který bude sloužit jako hlavní virtualizační platforma, a to jak pro nově pořízené technologie, tak pro současné. Server bude připojen optickou linkou 4x 10Gbit/s do páteřní sítě školy. Dodávka nových licencí operačních systémů a klientské přístupové licence jsou také součástí plnění.
Prodávající provede přesun virtuálních serverů a služeb ze stávajícího na nový server v rámci stejné virtualizační platformy a bude také proveden upgrade všech operačních systémů na nejnovější dostupné verze.
Bude nasazena ochranou nově pořízených technologií vůči výpadku elektrického proudu v podobě UPS
Dodávka licencí pro hypervizor není součástí projektu – bude použita technologie Hyper-V, která bude součástí dodávaného serverového operačního systému.
Aktuálně používaný systém zálohování bude nahrazen novým síťovým úložištěm „NAS“ s dostatečnou kapacitou pro ukládání provozních záloh. Zálohování bude řízeno pokročilým zálohovacím softwarem, který bude prostřednictvím virtualizačního hypervizoru zálohovat všechny virtuální servery. Zálohovací systém umožní zálohovat i fyzické servery a osobní počítače. Síťové úložiště NAS bude kvůli bezpečnému oddělení záloh umístěno mimo místnost serveru.
Licence operačních systémů musí umožnit využití implementovaných funkcionalit serverových řešení. Požadované licence desktopových operačních systémů musí umožnit začlenění stávajících počítačů pod kontrolu a centrální řízení adresářové služby Active Directory, ověřování přístupu k síti a poskytování potřebných informací pro systém centrálního logování.
Pro obvyklá zařízení využívané školami a určená k připojení do počítačové sítě (kategorie stolní a přenosné počítače, tiskárny, tablety a chytré telefony, ostatní síťová koncová zařízení) bude předvedena vzorová konfigurace a plné funkcionalita zařízení v síti, dále bude provedeno seznámení s vazbami zabezpečení sítě-konfigurace zařízení a demonstrováno logování provozu zařízení a činnosti jeho uživatele. Předvedení bude provedeno pro takový počet vzorků, aby byly pokryty významné odlišnosti vzorků v rámci kategorie z pohledu funkcí či potřebných konfigurací (např. tablety s OS Android a IOS).

5.4 Instalační a implementační služby v oblasti koncových zařízení

Součástí komodity je dodávka, instalace a konfigurace koncových zařízení potřebných pro vedení výuky.
U PC se bude jednat zejména o jejich zapojení a napojení na MS Active Directory
U projektorů se bude jednat o jejich montáž, napojení na zdroje signálu a dat, předvedení a ověření funkčnosti.

5.5 Školení

Prodávající provede pro každý typ zařízení a software odborné školení na obsluhu a práci s dodanými zařízeními, a to minimálně v rozsahu provozní dokumentace.
Školení bude pokrývat všechna zařízení a systémy všech komodit, dodávané v rámci plnění této specifikace, a to minimálně v rozsahu:

- běžných administrátorských činností pro implementované systémy
- standardní údržby systémů pro administrátory zadavatele

Školení dále zajistí seznámení pracovníků zadavatele se všemi podstatnými částmi plnění v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.
Minimální rozsah školení pro každé zařízení a software jsou 2 hodiny, není-li uvedeno jinak. Školení bude probíhat v sídle kupujícího. Počet školených osob kupujícího je stanovena na max. 3 osoby.

5.6 Plnění standardu konektivity škol

Předmět plnění dle této technické specifikace slouží k naplnění účelu dosažení standardu konektivity školy stanovenému na URL: https://www.edu.cz/digitalizujeme/standard-konektivity-skol/
Prodávajícího se v rámci realizace tohoto plnění zavazuje pro kupujícího dodat a nakonfigurovat technologie tak, aby jejich prostřednictvím bylo dosaženo standardu konektivity, a to v rozsahu, ve kterém jsou tyto technologie pro plnění standardu konektivity pořizovány.

Dále se prodávající zavazuje poskytnout kupujícímu součinnost a zejména konkrétní sestavení požadavků na plnění standardu konektivity z pohledu služeb **poskytovatele internetového připojení** tak, aby v návaznosti na nasazené technologie bylo možné u poskytovatele internetového připojení provést zbývající konfigurace k dosažení potřebného naplnění standardu konektivity dostupnému na výše uvedeném URL. Prodávající za tímto účelem poskytne kupujícímu až 5 hodin odborných konzultačních služeb, jejichž součástí bude písemné zpracování požadavků na změnu služeb a technologií na straně poskytovatele internetového připojení a dále konzultace k jejich nasazení.

Dále se prodávající zavazuje poskytnout kupujícímu součinnost a zejména konkrétní sestavení požadavků na plnění standardu konektivity z pohledu služeb **poskytovatele hostingu** webových stránek a emailů školy tak, by tyto služby byly zabezpečeny v rozsahu definovaném standardem konektivity, tedy zejména DNSSEC. Prodávající za tímto účelem poskytne kupujícímu až 5 hodin odborných konzultačních služeb, jejichž součástí bude písemné zpracování požadavků na změnu služeb a technologií na straně poskytovatele hostingu a dále konzultace k jejich nasazení.

Prodávající je dále povinen v rámci plnění standardu konektivity dostupném na výše uvedeném URL pro kupujícího navrhnout **Směrnici a další dokumentaci**, kterou standard konektivity vyžaduje a je ji potřeba předložit k prokázání jeho dosažení. Směrnice musí odpovídat minimálnímu rozsahu stanovenému standardem konektivity, zohledňovat nasazené technologie a zajistit synergii procesů stanovených touto směrnicí s nově vybudovaným a vybaveným technologickým prostředím školy.

Veškerou součinnost poskytovatele internetového připojení kupujícího zajišťuje kupující. Pro podání nabídky proto služby poskytovatele internetového připojení nevstupují jako součást plnění a není proto ze strany prodávajícího potřeba zajistit pro jeho nabídku potřebou přímou součinnost poskytovatele internetového připojení kupujícího.

V rámci plnění této specifikace nedochází k budování ICT kabelových rozvodů, které jsou samostatným plnění mimo plnění podle této dokumentace. ICT kabelové rozvody budou vybudovány a připraveny pro realizaci tohoto plnění.

Plnění Standardu konektivity škol, kterého musí být v rámci realizace plnění dle této specifikace dosaženo je mimo jiné definované v následující podobě (uvedeno ve sloupci komentář), které kupující užil jako stanovení cíle pro dotační žádost, ze které bude toto plnění kofinancováno:

Parametr	Plnění (ano/ne/ nerelevantní)	Komentář
Konektivita školy k veřejnému internetu (WAN) - povinné parametry		
Šíře pásma (bandwidth) odpovídající 0,25 Mbps/žák či student nebo 0,5 Mbps/koncové uživatelské zařízení a zároveň taková šířka pásma, která neomezuje provoz zařízení a uživatelů. Šíře pásma se vztahuje na počet žáků/studentů/koncových uživatelských zařízení v budově/areálu, kde se projekt realizuje	Ano	Tento parametr škola v současné době splňuje.
Vlastní nebo poskytovatelem přidělené veřejné IPv4 adresy.	Ano	Tento parametr škola v současné době splňuje.
Zajištění monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu koncovému zařízení v minimální délce 3 měsíců.	Ano	Tento parametr škola v současné době nesplňuje, proto bude v rámci projektu implementován systém "log management". Tím bude parametr naplněn.
Síťové zařízení podporující rate limiting, antispoofing, access listy - zařízení musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality.	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní síťové prvky (firewall, přepínače, WiFi AP) s požadovanými funkcemi. Tím bude parametr naplněn.
Schopnost snadné/automatické rekonfigurace pravidel firewallu (access listů) na základě identifikovaných útoků.	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní síťové prvky (firewall, přepínače, WiFi AP) s požadovanými funkcemi. Tím bude parametr naplněn.
Zajištění šifrovaného přístupu (SSL/TLS) a podepsání DNSSEC domén pro služby školy dostupné online (např. emailové služby, webové servery, studijní a ekonomické agendy atp.).	Ano	Tento parametr škola v současné době nesplňuje, proto bude v rámci projektu pořízen wildcard certifikát a bude provedena rozšířená konfigurace DNS serveru. Tím bude parametr naplněn.
Validující DNSSEC resolver na straně školy, nebo poskytovatele konektivity, nebo otevřeným DNSSEC validujícím resolverem	Ano	Tento parametr škola v současné době nesplňuje, proto bude v rámci projektu provedena rozšířená konfigurace DNS serveru. Tím bude parametr naplněn.

Software a firmware je aktualizován po dobu udržitelnosti projektu, jsou-li aktualizace k dispozici	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní síťové prvky (firewall, přepínače, WiFi AP) s požadovanými funkcemi. Tím bude parametr naplněn.
Poskytovatel konektivity je schopen zajistit kontaktní bod pro komunikaci, trvalý monitoring dostupnosti konektivity, realizovat blokování nežádoucí komunikace zahlcující nebo jinak omezující konektivitu a systémy školy na straně poskytovatele na základě požadavku školy.	Ano	Tento parametr škola v současné době splňuje
Konektivita školy k veřejnému internetu (WAN) - doporučené parametry		
Symetrické připojení (zajištění konektivity) bez agregace a omezení.	Ano	Tento parametr škola v současné době splňuje.
Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6, včetně zajištění dostupnosti online služeb školy na IPv6 adresách.	Ano	Tento parametr škola v současné době nesplňuje. Budou pořízeny aktivní prvky s podporou IPv6 a ve spolupráci s poskytovatelem internetu provedena konfigurace, tím bude parametr naplněn.
Poskytovatel konektivity je schopen zajistit funkci systému incident response, monitoring a aktivní notifikaci anomálií síťového provozu, zamezení podvržení zdrojových IP adres (anti-spoofing), funkci pro blokování nežádoucí komunikace zahlcující nebo jinak omezující konektivitu a systémy školy pro zamezení zahlcení linky (např. RTBH, FlowSpec, služby AntiDDoS řešení), detekci a zamezení amplifikačních útoků, zabezpečení směrování síťového provozu pomocí RPKI a konfigurace odmítnutí nevalidních prefixů.	Nerelevantní pro tento projekt	
Antivirová kontrola internetového provozu	Nerelevantní pro tento projekt	
Vnitřní konektivita školy (LAN a WLAN) - společné povinné parametry		
Systém správy uživatelů (Identity Management), tj. centrální databáze identit (LDAP, AD apod.) a její využití pro autentizaci uživatelů (žáci i učitelé) za účelem bezpečného a auditovatelného přístupu k síti, resp. službám. Využívání jednoho účtu více uživateli není povoleno (využívání tzv. anonymních účtů).	Ano	Tento parametr škola v současné době nesplňuje. Budou pořízeny aktivní prvky , server a serverový OS s podporou auditovatelného přístupu k síti a tím bude parametr naplněn.
Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém	Ano	Tento parametr škola v současné době nesplňuje, proto bude v rámci projektu implementován systém "log management". Tím bude parametr naplněn.

Systémy zálohování a obnovy dat serverové infrastruktury	Ano	Tento parametr škola v současné době nesplňuje, proto bude v rámci projektu pořízen zálohovací SW a NAS a tím bude parametr naplněn.
Systémy pro antivirovou ochranu počítačových systémů, antispamovou ochranu poštovních serverů	Ano	Tento parametr škola v současné době splňuje.
Vnitřní konektivita školy (LAN a WLAN) - povinné parametry pevné LAN		
Minimální konektivita koncových uživatelských zařízení 1000 Mbps fullduplex	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní prvky a natažena kabeláž, tím bude parametr naplněn.
Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení (např. IPS, IDS, Next Generation Firewall aj.), datových úložišť (NAS) 1000 Mbps fullduplex	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní prvky a natažena kabeláž, tím bude parametr naplněn.
Síťové prvky musí splňovat následující funkcionality: centrální směrovače a centrální přepínače (L2 i L3) s neblokující architekturou přepínacího subsystému (wire speed), management, podpora 802.1Q VLAN (možnost tvorby virtuálních sítí - VLAN), základní bezpečnostní prvky proti zneužití přístupu k síti [např. MAC based omezení (port-sec), 802.1X autentizace aj.].	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní prvky a natažena kabeláž, tím bude parametr naplněn.
Strukturovaná kabeláž pro připojení počítačových systémů a dalších zařízení (tiskárny, servery, AP aj.).	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní prvky a natažena kabeláž, tím bude parametr naplněn.
Páteřní rozvody mezi budovami v areálu, kde probíhá výuka nebo příprava na ni, realizovány prostřednictvím optických vláken nebo metalických kabelů. Vztahuje se na budovu/areál, kde se projekt realizuje.	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní prvky a natažena kabeláž, tím bude parametr naplněn.
Vnitřní konektivita školy (LAN a WLAN) - povinné parametry bezdrátové sítě WLAN		
Návrh topologie Wi-Fi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů.	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní prvky, natažena kabeláž a nainstalovány WiFi vysílače, tím bude parametr naplněn.
Zabezpečení minimálně AES šifrováním a standardem WPA2-Enterprise nebo WPA3-Enterprise, multi SSID, ACL pro filtrování provozu.	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní prvky, natažena kabeláž a nainstalovány WiFi vysílače, tím bude parametr naplněn.

Zajištění vzájemně oddělených sítí pro zaměstnance školy, žáky/studenty školy a externí zařízení (hosty).	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní síťové prvky (WiFi AP) s požadovanými funkcemi. V rámci nové WiFi sítě budou zřízené nové SSID sítě, které oddělí zaměstnance školy, žáky/studenty školy a externí zařízení (hosty).
Podpora mechanismu izolace uživatelů.	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní síťové prvky (WiFi AP) s požadovanými funkcemi. Tím bude parametr naplněn.
Podpora standardu IEEE 802.11ac (Wi-Fi 5) a případně novějších (Wi-Fi 6), současná funkce AP v pásmu 2,4 a 5 GHz a novějších protokolů a pásem.	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní síťové prvky (WiFi AP s podporou Wi-Fi 6) s požadovanými funkcemi. Tím bude parametr naplněn.
Vnitřní konektivita školy (LAN a WLAN) - společné doporučené parametry		
Logování provozu za účelem dohledatelnosti na úroveň koncového uživatele.	Ano	Tento parametr škola v současné době nesplňuje. Budou pořízeny aktivní prvky, server a serverový OS s podporou auditovatelného přístupu k síti, implementován systém "log management". Tím bude parametr naplněn.
Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty) a systému blokace Wi-Fi v určitém čase.	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní síťové prvky (WiFi AP) s požadovanými funkcemi. Řešení bude vybudováno na Captive portálu. Tím bude parametr naplněn.
Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací (např. aktivní zapojení do federovaného systému www.eduroam.cz).	Ano	Tento parametr škola v současné době nesplňuje, bude implementován systém EDUROAM.
Centralizovaná architektura správy Wi-Fi sítě (centrální řadič, centrální management, tzv. thin access pointy, popř. alespoň centrální řešení distribuce konfigurací s podporou automatického rozložení zátěže klientů, roamingu mezi spravované access pointy a automatickým laděním kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení).	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní síťové prvky (WiFi AP) s požadovanými funkcemi. Tím bude parametr naplněn.
Doporučená podpora pro ověřování uživatelů oproti databázi účtů [např. pomocí protokolu IEEE 802.1X vůči centrální evidenci uživatelů (např. LDAP, MS AD) nebo pomocí Captive portalu].	Ano	Tento parametr škola v současné době nesplňuje. Nově pořízené technologie (switche, Wi-Fi AP) škole umožní vybudování RAIDUS serveru a captive portálu. Tím bude parametr naplněn.

Propojení aktivních prvků a důležitých systémů (např. Servery, NAS, propojení budov) rychlostí 10 Gbps, včetně uplinku.	Ano	Tento parametr škola v současné době nesplňuje, projekt počítá s pořízením všech klíčových zařízení s možností připojení 10Gbit. Tím bude parametr naplněn.
Doporučené bezpečnostní prvky projektu		
Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3917 - IPFIX nebo ekvivalent)	Nerelevantní pro tento projekt	
Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie.	Ano	Tento parametr škola v současné době nesplňuje. Budou pořízeny aktivní prvky, server a serverový OS s podporou auditovatelného přístupu k síti, implementován systém "log management", firewall Next generation. Tím bude parametr naplněn.
Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management).	Ano	Tento parametr škola v současné době nesplňuje, proto bude v rámci projektu implementován systém "log management". Tím bude parametr naplněn.
Systémy pro monitorování funkčnosti síťové a serverové infrastruktury.	Nerelevantní pro tento projekt	
Zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu.	Ano	Tento parametr škola v současné době nesplňuje. Budou pořízeny aktivní prvky s požadovanou funkcionalitou, tím bude parametr naplněn.
Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk aj.).	Nerelevantní pro tento projekt	
Nástroje pro centrální správu a audit ICT prostředků.	Nerelevantní pro tento projekt	
Podpora vzdáleného přístupu (VPN).	Ano	Tento parametr škola v současné době nesplňuje. Budou pořízeny aktivní prvky s požadovanou funkcionalitou, tím bude parametr naplněn.
Zavedení více-faktorové autentizace.	Nerelevantní pro tento projekt	

Povinným akceptačním kritériem bude prokázání naplnění požadavků Standardu konektivity škol dle manuálu uveřejněného na Standard konektivity a bezpečnosti škol - edu.cz včetně úspěšného provedení a doložení testu na https://www.standardkonektivity.cz/. Prokázání naplnění požadavků poskytne prodávající v písemné formě vhodné jako přílohu k Závěrečné zprávě o realizaci projektu.

Kupující upozorňuje, že pro dosažení naplnění standardu konektivity jsou potřeby i služby poskytovatele internetového připojení a hostingu kupující, pro něž prodávající písemně poskytne potřebné požadavky na konfigurace. Prodávající proto v rámci svého plnění musí postupovat tak, aby tyto třetí strany měli odpovídající časový prostor v rámci jejich součinnosti zajišťované kupujícím tyto

konfigurace nastavit a prodávající pak mohl jako pro kupujícího zajistit komplexní výstupy naplnění standardu konektivity, které následně kupujícímu poslouží jako výstup pro prokázání naplnění požadavků jím realizovaným projektem.

6 Záruky a servisní podmínky

6.1 Požadavky na záruky a servisní podmínky

(1) Zadavatel uvádí u jednotlivých komodit, resp. jejich částí požadovanou min. záruku, popř. podporu. Uváděné parametry byly průzkumem trhu zjištěny jako standardní, tj. poskytovány výrobci jako součást standardní dodávky a ceny. Není-li záruka části uvedena, je pro tuto část požadována záruka min. 24 měsíců.

(2) Zadavatel požaduje bezplatný (zahrnutý v ceně zakázky) přístup k aktualizacím software a firmware dodaných komodit minimálně po dobu záruky.

(3) Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro zadavatele.

(4) Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.

(5) Není-li uvedeno u konkrétní komodity jinak, požaduje zadavatel provedení záruční opravy do pěti pracovních dnů.

(6) Po dobu 60 měsíců od předání díla jako celku do plného provozu, musí dodavatel nebo výrobce všech zařízení garantovat běžnou dostupnost náhradních komponentů a dostupnost servisu.

(7) Dodavatel ve své nabídce výslovně uvede všechny podmínky záruk.

6.2 Požadavky na zabezpečení provozu

(1) Z důvodu zajištění udržitelnosti projektu po dobu 60 měsíců a zajištění bezpečnosti provozu požaduje zadavatel zajištění poskytnutí podpory softwarových produktů.

(2) Podpora je požadována minimálně v rozsahu potřebném pro zajištění bezpečného provozu dodaných systémů.

(3) V případě požadavku zadavatele je uchazeč povinen podporu v tomto rozsahu poskytnout. Cenu poskytnutí uvede dodavatel v Příloze č. 1 Kupní smlouvy – Kalkulace nabídkové ceny do určených polí v listu Provoz.

1 Technická specifikace zadavatele (kupujícího)

Zadavatel požaduje dodávku jednotlivých komponent dle této technické dokumentace včetně příslušenství v níže uvedené minimální specifikaci.
Musí se jednat o zařízení nová, nepoužitá, nerepasovaná a určená pro prodej v České republice.
Součástí dodávky níže uvedených technologií budou i dále uvedené služby.
Součástí dodávky bude dále dodávka dokumentace a nezbytné zaškolení administrátorů v prostředí kupujícího k běžnému provozu a ovládání dodaných technologií včetně specifik a konfigurace provedené v prostředí kupujícího.
Nabízené zboží musí být standardní, běžně dostupné a určené k produkčnímu použití.
Není dovoleno použití beta-verzí, kódu s custom úpravami či neoficiálních verzí.
Veškeré nabízené zboží musí být pokryto oficiálním supportem, přičemž požadavek na provedení bezplatného servisního zásahu musí být možné kdykoliv vznést přímo na výrobce zařízení.
Veškeré deklarované funkce a technické parametry nabízeného zboží musí být dostupné nejpozději dnem podání nabídky.
Deklarované funkce a technické parametry nabízeného zboží musí být ověřitelné prostřednictvím oficiálních datasheetů, release notes či manuálů vydaných výrobcem.
Užité pojmy níže:

- NBD – další pracovní den, tzn. například realizace opravy zařízení nejpozději další pracovní den od nahlášení
- x BD – x pracovních dnů, tzn. například realizace opravy zařízení nejpozději poslední pracovní den dané lhůty od nahlášení
- on-site – realizace například opravy zařízení v místě dodávky

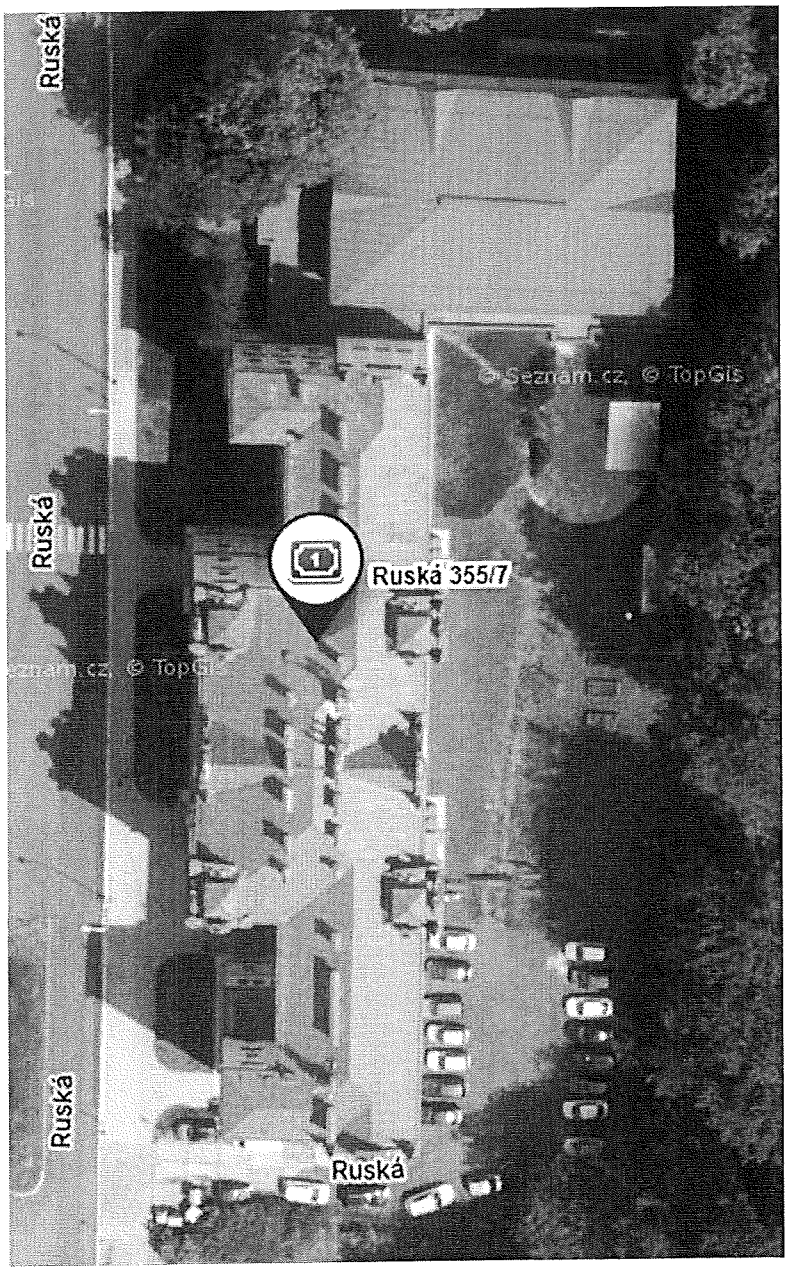
Propojení zařízení – SFP moduly a kabely
Všechny dodané technologie musejí být v rámci dodávky propojeny odpovídajícím způsobem a technologií, tedy zejména pro všechny síťové karty jednotlivých zařízení musejí být dodány i SFP a obdobné moduly a kabely do serverovny kupujícího, které takové propojení v kvalitě požadované u každého ze zařízení umožní. V případě 10Gbit karet musí být dodány SFP prvky a kabely umožňující využití této maximální rychlosti karty, v případě jiných rychlostí toto pravidlo musí být dodrženo stejně.

Počty jednotlivých komponent, které jsou předmětem tohoto plnění jsou uvedeny v samostatném souboru s názvem „Cenová tabulka".

Obsah

2 Popis současného stavu

(1) Areál Gymnázia a obchodní akademie Mariánské Lázně, příspěvkové organizace je umístěn na adrese Ruská 355/7, 35301 Mariánské Lázně a je tvořen hlavní budovou školy a přístavkem s tělocvičnou, viz. obrázek. V současné době navštěvuje školu téměř 430 žáků a škola má 47 zaměstnanců.



(2) Realizace plnění bude probíhat ve všech využívaných objektech.

(3) Současný stav ICT školy neodpovídá Standardu konektivity škol (dále jen Standard konektivity), a současným nárokům na výkon, bezpečnost a centralizovanou správu počítačové sítě. Počítačová síť byla budována postupně, staří a technické úroveň používaných prvků se výrazně liší. Síťové pokrytí na úrovni metalických kabelů Cat5 bylo budováno a rozšiřováno postupně podle aktuálních potřeb a finančních prostředků školy. Bezdrátové připojení bylo realizováno v roce 2021 na úrovni standardu

WiFi 5 pro potřeby pokrytí aktuálních potřeb a s ohledem na omezené finanční možnosti, bez rezerv pro budoucí rozvoj. Část použitých aktivních prvků sítě je již technicky i morálně zastaralých a výrobci nepodporovaných (nebo jen omezeně). Chybí významná provázanost a centralizovaná správa infrastruktury.

(4) Kabelové rozvody byly provedeny kabely Cat5e. Pokrytí potřebných prostor budov metalickými rozvody je nedostatečné a neumožňuje připojovat do sítě další zařízení (koncová zařízení, IoT a bezpečností prvky (kamery apod.) a síť rozvíjet např. doplňováním WiFi přístupových bodů. Nedostatek přípojných míst je na některých místech řešen „rozbočováním" sítě malými přepínači bez managementu, jejichž použití dále komplikuje správu celé sítě a snižuje její robustnost, stabilitu a bezpečnost. Kabeláž je uložena převážně v lištám, občas „pod kobercem".

(5) Aktuálně využívaný server byl dodán v roce 2020/09. Výkonem a kapacitou server vyhovuje aktuálním požadavkům, ale není schopen splnit všechny požadavky systému splňujícího požadavky Standardu konektivity.

(6) Server je aktuálně připojen rychlostí 10Git/s do páteřního switche ve spodním rozvaděči.

(7) V hlavní budově je umístěn další páteřní switch a propojení dvou páteřních switchů je provedeno optickým kabelem rychlostí 10Gbit/s. Optický kabel mezi spodním rozvaděčem (u tělocvičny) a horním rozvaděčem (učebna 316) je aktuálně veden nepoužívaným komínovým průduchem.

(8) Propojení stanic i serverů je zajištěno přepínači 1 Gb/s bez možnosti pokročilé správy. Hlavní aktivní prvky jsou umístěné v několika datových rozvaděčích. Aktivní prvky nesplňují požadavky na zabezpečení přístupu do LAN pomocí 802.1X.

(9) Internetové připojení je realizováno společností ČezNet optickým přípojem s rychlostí 200Mb/s symetricky včetně IPv6 konektivity. Rychlost připojení tak převyšuje požadavek Standardu konektivity škol – 107,5 Mbps (430 žáků x 0,25 Mbps).

(10) Škola má přiděleny veřejné IP adresy IPv4 (7 adres), včetně IPv6 veřejných adres s rozsahem :/ 56 adresy. Škola nemá v současné době validující DNSSEC resolver na straně školy, neprovádí pokročilý monitoring provozu. Škola provozuje 2 domény – goaml.cz a goaml.eu

(11) Škola provozuje Wifi síť, které pokrývá pouze část školy. Byla realizovaná v roce 2021 a splňuje technologické požadavky kategorie WiFi 5. Tato WiFi síť slouží pro potřeby zaměstnanců i žáků školy. Síť má více SSID. Síť pro zaměstnance školy je chráněná silným heslem a má přístup k systémovým prostředkům školy. Síť pro žáky je chráněna heslem a uživatelé této sítě mají povolený pouze přístup do internetu. Síť je centrálně spravovaná. Použité prvky nepodporují aktuální bezpečnostní standardy (WPA3 apod.), ani pokročilé funkce optimalizace rádiového provozu a obsluhy připojených klientů.

(12) Zabezpečení přístupu k internetu využívá pouze NAT na hraničním prvku – routeru. Nejsou využívány pokročilé bezpečnostní funkce např. URL filtrace, antivirová kontrolou a detekce průniků.

(13) Škola provozuje jeden fyzický server s virtualizací. Jako hypervisor pro virtualizaci se používá řešení VMWare 6.5 Je provozováno několik různorodých operačních systémů. Virtuální Windows server 2019 je využíván 4x pro Active Directory a sdílení souborů (zajišťuje DNS v síti), Bakaláře, Terminál server, a server Docházky. Na serverech jsou dále provozovány 3 virtuální Servery Linux v různých verzích - jednak pro webové stránky školy a různé projekty, dále pak pro odesílání mailů ze starších tiskových zařízení, které nepodporují dvoufaktorové ověřování a v neposlední řadě pak pro starší projekty jako Moodle.

(14) Zálohovaní serveru řídí prostředky operačního systému a systému záloh pomocí hypervisoru ve spolupráci se software Synology Active Bussiness Backup. Zálohy jsou ukládány na síťový server NAS

umístěný odděleně od serveru. Kapacita NAS je dostatečná pro zálohování současného objemu dat a realizaci pokročilé ochrany záloh před kompromitací např. snapshoty či obdobnou technologií.

(15) Škola disponuje centrální databází uživatelských identit Active Directory a využívá ji pro ověřování identity všech uživatelů přistupujících k síťových prostředků.

(16) Přístup do počítačů (resp. operačních systémů) je řízen převážně ověřováním vůči doméně Active Directory. Pouze malá část (méně než 10%) využívá ověřování lokálními uživatelskými účty.

(17) Hlavní softwarovou platformou serverů i uživatelských počítačů jsou operační systémy společnosti Microsoft a OpenSuse. Na koncových počítačích učitelů i žáků jsou používány převážně operační systémy Windows 10 a vyšší s podpory domény Active Directory. Škola provozuje aktuálně téměř 190 zařízení. Správa životního cyklu operačních systémů a aplikačního vybavení se provádí manuálně. Ochrana počítačů před škodlivým software je zajišťována systémem ESET Internet Security.

(18) Škola využívá a prostřednictvím internetu vzdáleně zpřístupňuje webové aplikace – internet školy (https://www. Goaml.cz), školský informační systém Bakaláři (https://bakalari.goaml.cz/). Aplikace jsou publikovány na IPv4 adresách, jsou dostupné šifrovaným protokolem https zabezpečeným certifikáty vydanými veřejnými certifikačními autoritami.

(19) Škola využívá aktuálně 18 tabletů, 4 síťové tiskárny a 170 počítačů pevných počítačů a notebooků. Plánovaný cílový počet během následujících 5 let může dosáhnou počtu 250. Průměrné stáří stávajících počítačů přesahuje 5 let. Počítače jsou vybaveny systémem Windows verze 10 a 11 ve verzi podporující doménu Active Directory.

(20) Od 1.11.2024 škola nově využívá: Licence Microsoft v programu EES CZESHA pro školy

M365 A3 Unified Edu Sub Per User	**39 licencí**
Win Server Standard Core ALng LSA 16L	**2 licencí**
M365 A3 Unified Edu Sub Student Use Benefit Per User	**780 licencí**

3 Popis cílového stavu a specifikace předmětu plnění

Základní požadavky na technické řešení

(1) V rámci projektu bude maximalizováno využití technických a systémových prostředků pořízených v předchozích projektech nebo vlastní investicí formou sdílení těchto prostředků tam, kde je to technicky, provozně a z pohledu bezpečnosti vhodné a možné.

(2) Cílem projektu je zvýšení bezpečnosti a související modernizace IT infrastruktury, aby implementací projektu byly naplněny Standardy konektivity škol[1] (dále jen Standard konektivity) a rozšířena funkčnosti ICT prostředí zapojených škol. Dílčí cíle dle jednotlivých komodit jsou specifikovány následovně:

Označení	Komodita
A	Rozvody LAN
B	Zabezpečení LAN a Wifi
C	Centrální logování
D	Server, zálohování a licence operačních systémů
E	Koncová zařízení

(3) Je požadováno řešení zachovávající a rozvíjející současné softwarové platformy Microsoft pro zachování kompatibility se stávajícími systémy a aplikacemi. Přechod na jinou platformu by způsobil zásadní uživatelské a provozní potíže.

(4) Je požadována unifikace jednotlivých komodit (tj. jejich realizace stejnými prostředky) pro všechny části z důvodu jednotné správy celého prostředí a odpovídající minimalizace provozních nákladů.

(5) Pokud prodávající (dále jen jako „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.

(6) 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 ceny za pořízení a provoz v rámci příslušných částí stanovené v Zadávací dokumentaci.

(7) Kupující (dále též jako „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.

(8) Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky:

- jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
- mají plnou záruku od výrobce,
- mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
- obsahují všechny nezbytné licence na používání příslušného softwaru,
- jsou v databázi výrobce uvedeny jako prodaná kupujícímu,
- jsou určeny pro provoz v České republice.

[1] Viz. aktuální verze https://www.edu.cz/digitalizujeme/standard-konektivity-skol/

(9) 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.

(10) Veškerá realizační dokumentace dodávaná v rámci 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.

4 Specifikace dodávaných technologií

Zadavatel požaduje, aby nabízená řešení měla požadované funkce již v době podání nabídky, nikoliv aby se jednalo o budoucí funkce plánovaných verzí software pro nabízené řešení.

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

Označení jednotlivých částí koresponduje s členěním ve Výkazu výměr.

Komodita A - Rozvody LAN		
Část	**Parametr**	**Popis povinného parametru**
Kabelové rozvody včetně příslušenství	Popis	Kabelové rozvody včetně příslušenství a souvisejících služeb dle podrobného výkazu výměr
	Záruka	Kabelové rozvody 10 let, rozvaděče 24 měsíců

Komodita B - Zabezpečení LAN a Wifi		
Část	**Parametr**	**Popis povinného parametru**
B001 **Perimetrový firewall 1ks**	Provedení	Umístitelné do racku
	HW parametry	Počet síťových rozhraní LAN RJ45 1 Gb - min 14x nebo jiná technicky kvalitnější kombinace portů (např. 2x 10Gb a 6x 1Gb)
		Počet rozhraní USB pro připojení ext. modemu - min. 1x
	Výkon	Propustnost firewallu min. 20 Gb/s nezávisle na velikosti paketu
		Propustnost firewallu - min. 15 Mpps (pps - paketů za sekundu)
		Počet FW politik min. 10 000
		Počet současných otevřených spojení - min 1,5 M
		Propustnost VPN - min. 11,5 Gbps
		Propustnost IPS - min 2,6 Gbps
		Propustnost antiviru - min. 1 Gbps
	Funkce	Režim vysoké dostupnosti - Active Active, Active Passive, Clustering
		Režim fungování L2 – transparentní režim, L3 – NAT/Router
		Podpora multicast, vytváření politiky pro multicast routování
		Podpora VPN: IPSec, SSL (portálový režim, tunelový režim), IPSEC (IKE, manual key, certifikát, gateway to gateway, hub and spoke, dial up konfiugrace, internet browsing konfigurace, podpora vice tunelů – redundantní VPN
		Podpora IPv6
		Podpora virtualizace (min. 10 virtuálních kontextů - firewallů)
		Podpora dynamických routovací protokolů - OSPF, PPTP, L2TP, GRE
	Firewall	Možnost nastavovat firewall politiku na základě geografických údajů.
		Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru Active Directory.
		Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offload.
		Podpora centrální NATovací tabulky
	Filtrační funkce	Možnost výběru mezi file based režimem (buffer) nebo flow based (inspekce on-the-fly)
		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)
		Email filter – antispamová a antivirová inspekce elektronické pošty

Komodita B - Zabezpečení LAN a Wifi		
		Intrusion Protection System – detekce útoků založena na signaturové části a na anomálním filtru, možnost vytvářet vlastní signatury.
		Web Filter – 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.
		Application Control – detekce, monitoring, povolení či zakázání vice než 2000 síťových aplikací na základě signatury dané aplikace, nikoliv dle portu.
		Kontrola komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S)
		DoS Policy prevence proti základním útokům typu DoS, syn proxy
	Ověřování uživatelů	LDAP, Active Directory, Radius, TACACS+, Ověřování na základě certifikátu
		Podpora silné autentizace uživatelů – integrovaná podpora generátoru jednorázových hesel (OTP) – Token pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů
		Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření.
	Dynamické routování	RIP, BGP, OSPF, IS-IS
		Policy routing
		Traffic Shaping, QoS s podporou DSCP markování a ToS
		Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu
		WAN optimalizace (optimalizace vybraných protokolů, byte chaching), Web Cache, Explicitní Proxy, Reverzní prózy, WCCP
	Reporty	Integrované logování a reporting, možnost vytváření vlastních reportů
	SFP+ moduly a patch cordy	Součástí dodávky jsou potřebné originální SFP+ moduly a optické/metalické propojovací kabely pro realizace díla.
	Záruka	Záruka výrobce min. 60 měsíců v režimu 24x7 na HW, OS, firmware a kompletní bezpečnostní SW. SW musí obsahovat IPS, AV, Web Filtering a Antispam aktualizace.
B002 **Centrální přepínač školy 1x**	Základní parametry	L2/L2+ přepínač v rackovém provedení max. 1U
	Porty	Min. 16x 10 Gb SFP+, vyhrazený samostatný LAN port pro management
	Propustnost	propustnost min. 300 Gbps
	Agregace portů	podpora LACP
	Správa	správa prostřednictvím kontroléru s plnou integrací (tj. kompletní správa prostřednictvím kontroléru a vyčítaní všech statusů do něj, vzdálený upgrade firmwaru z kontroléru)
	Podpora protokolů	podpora IPv6, Storm control, Spanning tree protocol
	VLAN	podpora VLAN, min. 500 aktivních VLAN současně (VLAN Group)
	Ověřování uživatelů a zařízení	podpora 802.1X
	MAC	podpora min. 20 000 MAC adres pro použití jako centrální switch (router)
	Routing	podpora statického routingu, min. 16 IPv4/IPv6 interface
	Port management	Rozšířený port management: VLAN, 802.1X autorizace, Radius VLAN, mirroring, agregace portů, pojmenování portů
	Napájení	interní redundantní zdroje (min 2)
	Monitoring a správa	plná podpora CLI, SSH, SNMP, syslog, sFlow, web rozhraní
	Záruka	min. 60 měsíců poskytovaná výrobce zařízení, a to včetně nároku na nové verze firmware
	Společné parametry	
B003 **Přístupové přepínače 8 ks**	Základní parametry	L2+ přepínač v rackovém provedení max. 1U
	Porty	min. 24x 10/100/1000Base-T RJ-45 porty + min. 4x 10 Gb/s SFP+ porty
	Propustnost	přepínací kapacita min. 120 Gb/s
	Podpora protokolů	podpora IPv6, Storm control, Spanning tree protocol
	Správa	správa prostřednictvím kontroléru s plnou integrací (tj. kompletní správa prostřednictvím kontroléru a vyčítaní všech statusů do něj, vzdálený upgrade firmwaru z kontroléru)
	Port management	rozšířený port management: VLAN, 802.1X autorizace, Radius VLAN, mirroring, agregace portů, pojmenování portů
	VLAN	podpora VLAN, min. 500 aktivních VLAN současně (VLAN Group)
	Ověřování uživatelů a zařízení	plná podpora 802.1X
	Záruka	min. 60 měsíců poskytovaná výrobce zařízení, včetně nároku na nové verze firmware
	Specifické parametry	

Komodita B - Zabezpečení LAN a Wifi		
B004 Přístupové přepínače s PoE 5 ks	Základní parametry	L2+ přepínač v rackovém provedení max. 1U
	Porty	min. 24x 10/100/1000Base-T RJ-45 porty + min. 4x 10 Gb/s SFP+ porty
	PoE	Všechny RJ-45 porty s podporou PoE+ napájení dle 802.3at, celkový PoE výkon min. 380W
	Propustnost	přepínací kapacita min. 120 Gb/s
	Podpora protokolů	podpora IPv6, Storm control, Spanning tree protocol
	Správa	správa prostřednictvím kontroléru s plnou integrací (tj. kompletní správa prostřednictvím kontroléru a vyčítaní všech statusů do něj, vzdálený upgrade firmwaru z kontroléru)
	Port management	rozšířený port management: VLAN, 802.1X autorizace, Radius VLAN, mirroring, agregace portů, pojmenování portů
	VLAN	podpora VLAN, min. 500 aktivních VLAN současně (VLAN Group)
	Ověřování uživatelů a zařízení	plná podpora 802.1X
	Záruka	min. 60 měsíců poskytovaná výrobce zařízení, včetně nároku na nové verze firmware
	Specifické parametry	
B005 Kontrolér 1 ks	Základní funkce	Kontrolér je určený pro řízení a správu switchů a WiFi přístupových bodů. Může být dodán jako samostatné HW zařízení nebo virtuální nebo softwarové řešení
	Počet spravovaných zařízení	min. 80 access pointů a 20 switchů
	Licence	trvalá, žádné licenční poplatky
	LAN porty	min. 1x port 10/100/1000Base-T RJ45 pro připojení do sítě
	Rozhraní	uživatelsky příjemné grafické rozhraní, web rozhraní
	Možnosti konfigurace	hromadná (dávková) konfigurace
	Informace o provozu	statistiky provozu, online zobrazování událostí a upozornění
	Přístupy pro hosty	generovaní voucherů pro přístup – 1, 4, 8hodin, 1, 7dní s možností tisku na běžné kancelářské tiskárně – Hotspot, Guest portal
	Autorizace uživatelů	autorizace uživatelů ze serveru Microsoft Active Directory
	Upgrade	upgrade firmware v zařízeních
	Sledování provozu	vytváření mapy sítě (umístění zařízení a jejich status – online)
	Zálohování	zálohovaní konfigurace v online provozu
	Běh na L3 sítí	běh na L3 sítí (tj. spravované prvky se nemusejí nacházet jen v dané broadcast doméně)
	Politiky pro skupiny uživatelů	ACL a Group Policy pro provozní údaje pro dané skupiny uživatelů – šířka přenosového pásma, časové rozlišení provozu, systém autorizace
	Provedení	instalace do 19" rozvaděče
	Záruka	min. 60 měsíců poskytovaná výrobce zařízení, a to včetně nároku na nové verze firmware
	Specifické parametry	
B006 WiFi přístupové body vnitřní (AP) 53 ks	Základní funkce	Přístupový bod (AP) standardu Wi-Fi 6 včetně montážního materiálu na stěnu nebo strop
	Frekvence	podpora WiFi 6 protokolu 802.11ax v obou pásmech 2,4 GHz a 5 GHz
	Anténní systém	min. 4 integrovaných antény (2 antény min. 3dBi pro 2,4GHz a 2 antény min. 5dBi pro 5GHz)
	Přenosové rychlosti	přenosová rychlost min. 574 Mb/s v pásmu 2,4 GHz a 2400 Mb/s nebo vyšší v pásmu 5 GHz
	Standardy	podpora 802.3at, 802.11n, 802.11ax, 802.1x včetně přiřazování do VLAN, podpora WiFi kanálu s šířkou 160 MHz
	Výstupní výkon	výstupní výkon min. 20 dBm v pásmu 2,4 GHz a min. (20-23 dBm – 100 až 200 mW), pokud bude pokrytí WiFi signálem v pásmu 5 GHz dostatečné pro spolehlivou práci všech připojených klientů
	Ladění kanálů	automatické ladění Wi-Fi kanálů a možnost detekce s reakcí na non-wifi rušení
	Multi SSID	podpora vysílání min. 6 SSID (WiFi sítí) v každém pásmu současně, podpora přiřazení každého SSID samostatné VLAN
	Provedení	provedení umožňující montáž na strop i stěnu, včetně držáku pro montáž
	Porty	min. 1x Gigabit Ethernet RJ-45 port pro připojení do sítě, s podporou aktivního PoE napájení dle normy 802.3af nebo 802.3at
	Šifrování	podpora WPA3 Personal/Enterprise šifrování
	Bezpečnost	autorizace uživatelů pomocí 802.1X
	Konfigurace	plná konfigurace z kontroléru
	Indikace	indikace provozního stavu pomocí LED
	Upgrade firmware	vzdálený upgrade firmware z kontroléru

Komodita B - Zabezpečení LAN a Wifi		
	Správa frekvenčního pásma	přechod klientů (roaming) mezi AP, automatické rozkládání zátěže mezi AP
	Záruka	min. 60 měsíců poskytovaná výrobce zařízení, včetně nároku na nové verze firmware
B007 WiFi přístupový bod venkovní (AP) 1 ks	Základní funkce	Přístupový bod (AP) standardu Wi-Fi 6 určený pro venkovní provoz, včetně montážního materiálu na sloup
	Frekvence	podpora WiFi 6 protokolu 802.11ax v obou pásmech 2,4 GHz a 5 GHz
	Anténí systém	min. 4 integrovaných antény (2 antény min. 3dBi pro 2,4GHz a 2 antény min. 5dBi pro 5GHz)
	Přenosové rychlosti	přenosová rychlost min. 574 Mb/s v pásmu 2,4 GHz a 1201 Mb/s v pásmu 5 GHz
	Standardy	podpora 802.3at, 802.11n, 802.11ax, 802.1x včetně přiřazování do VLAN
	Výstupní výkon	výstupní výkon min. 20 dBm v pásmu 2,4 GHz a min. 26 dBm v pásmu 5 GHz s možností regulace
	Ladění kanálů	automatické ladění Wi-Fi kanálů a možnost detekce s reakcí na non-wifi rušení
	Multi SSID	podpora vysílání min. 6 SSID (WiFi sítí) v každém pásmu současně, podpora přiřazení každého SSID samostatné VLAN
	Provedení	provedení umožňující montáž na stožár nebo na stěnu, včetně držáku pro montáž
	Porty	min. 1x Gigabit Ethernet RJ-45 port pro připojení do sítě, s podporou aktivního PoE napájení dle normy 802.3af nebo 802.3at
	Šifrování	podpora WPA3 Personal/Enterprise šifrování
	Bezpečnost	autorizace uživatelů pomocí 802.1X
	Konfigurace	plná konfigurace z kontroléru
	Indikace	indikace provozního stavu pomocí LED
	Upgrade firmware	vzdálený upgrade firmware z kontroléru
	Správa frekvenčního pásma	přechod klientů (roaming) mezi AP, automatické rozkládání zátěže mezi AP
	Odolnost	odolnost proti vlivu počasí (možnost použít AP přímo ve venkovním prostředí, tj. odolnost proti vodě, dešti, prachu, větru apod.)
	Provozní teploty	Nejméně v rozsahu -30°C až +60°C
	Záruka	min. 60 měsíců poskytovaná výrobce zařízení, včetně nároku na nové verze firmware
	Specifické parametry	
B008 Optické prvky	SFP+ modul	16 ks modulu SFP+ 10 Gb, SM, BiDi, 10 km – kompatibilní s nabízenými přepínači, LC konektor
	SFP modul	2 ks SFP modul, SM, kompatibilní s nabízenými přepínači, LC konektor
	DAC kabely	9 ks DAC kabelů pro SFP+ rozhraní, 2m, kompatibilní s dodanými aktivními prvky
	Optické patch kabely	18 ks kabel SM s konektory LC-SC, délka 3 m pro připojení přepínačů do optických tras
	Záruka	36 měsíců
B009 Systém 802.1X Eduroam	Popis	Instalace a konfigurace systému 802.1X pro zajištění autentizace uživatelů připojených přes LAN a WiFi prostředky do počítačové sítě školy. Systém je založený na protokolu RADIUS a je integrovaný s Active Directory. Připojení do federovaného systému Eduroam.
B010 Přepínač 1 ks	Základní parametry	L2+ přepínač v rackovém provedení max. 1U
	Porty	min. 8x 10/100/1000Base-T RJ-45 porty + min. 2x 1 Gb/s SFP porty
	Propustnost	přepínací kapacita min. 20 Gb/s
	Podpora protokolů	podpora IPv6, Storm control, Spanning tree protocol
	Správa	správa prostřednictvím kontroléru s plnou integrací (tj. kompletní správa prostřednictvím kontroléru a vyčítaní všech statusů do něj, vzdálený upgrade firmwaru z kontroléru)
	Port management	podpora VLAN, min. 500 aktivních VLAN současně (VLAN Group)
	Ověřování uživatelů a zařízení	plná podpora 802.1X
	Záruka	min. 60 měsíců poskytovaná výrobce zařízení, včetně nároku na nové verze firmware

Komodita C - Centrální logování, monitoring síťového provozu		
Část	**Parametr**	**Popis povinného parametru**
C001 Systém pro sběr a správu logů a	Požadavky na systém pro centralizovanou správu logů, událostí a strojových dat	Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware.
		Veškerá konfigurace systému se musí provádět v grafickém rozhraní jednotné uživatelské webové konzole. Systém poskytuje podporu pro vizuální programování pro všechny kroky zpracování strojových dat. Ve webové konzoli se nepřipouští konfigurace za využití skriptů, maker nebo textových konfiguračních polí, do kterých se složité textové skripty/makra vkládají.

Komodita C - Centrální logování, monitoring síťového provozu		
monitoring síťového provozu 1x		Systém umožňuje dopsání parserů pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému - Uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na vytváření zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů v jednotném ovládacím grafickém webovém rozhraní viz bod č. 1. Vytváření a testování parserů nesmí mít vliv na provoz systému. Pro psaní parserů nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Požadujeme předložit příslušnou dokumentaci k vytváření parserů a testování jejich funkčnosti.
		Systém umožňuje v grafickém rozhraní vizuálního programovacího jazyka snadno provádět třídění a značkování vstupních dat pro jejich další zpracování. Nepřipouští se nastavování třídění vstupních dat ve formě skriptu/makra zobrazeného v textovém okně. Předložte příslušný odkaz na dokumentaci popisující funkčnost třídění vstupních dat.
		Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém musí umožňovat příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále požadujeme podporu sběru strojových dat z databází s nastavením v grafickém menu systému minimálně pro databáze MSSQL, MySQL, Oracle a PostgreSQL a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta. Předložte detailní komunikační matrici s popisem všech použitých protokolů a portů pro nabízený systém a dokumentaci k nastavení sběru z databází v grafickém rozhraní systému.
		Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv. Integrované parsery systému automaticky přidávají ke zprávám, kterých se to týká, meta informace o jaký druh zprávy se jedná, minimálně požadujeme rozlišení těchto druhů zpráv: úspěšné přihlášení, neúspěšné přihlášení, odhlášení, konfigurační změna, značka/tag. Tyto meta informace musí být možné přidávat i v uživatelsky definovaných parserech.
		Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv. Integrované parsery systému automaticky přidávají ke zprávám, kterých se to týká, meta informace o jaký druh zprávy se jedná, minimálně požadujeme rozlišení těchto druhů zpráv: úspěšné přihlášení, neúspěšné přihlášení, odhlášení, konfigurační změna, značka/tag. Tyto meta informace musí být možné přidávat i v uživatelsky definovaných parserech.
		Hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a standardizovat alespoň na tyto základní druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými čísly je pak možné při prohledávání dat provádět matematické operace (součty všech hodnot, průměry, nejmenší/největší hodnota apod.).
		Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, které vzniká v okamžiku přijetí logu systémem a kterým se systém defaultně řídí.
		Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.
		Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.
		Systém nesmí v žádném případě umožnit mazání nebo modifikování již uložených logů v rámci požadované retence. A to ani libovolnou konfigurační změnou - administrátorovi s nejvyššími oprávněními k navrhovanému systému. Každý zpracovaný log musí mít dohledatelný unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.
		Systém musí umožňovat konfiguraci filtrace nerelevantních událostí v grafickém rozhraní vizuálního programovacího jazyka. Pro psaní filtrace nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Předložte odkaz na dokumentaci popisující způsob filtrování nerelevantních událostí.
		Systém provádí konsolidaci logů na interním storage logovacího systému.
		Systém umožňuje snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj musí být integrální součástí navrhovaného systému a musí se obsluhovat v jednotném rozhraní nabízeného produktu. Předložte link nebo pdf popisující způsob vytváření reportů.
		Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky.
		Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele.
		Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele.

Komodita C - Centrální logování, monitoring síťového provozu		
		Systém podporuje nativní získávání logů z Office365/Microsoft365 prostředí bez ohledu na použitou licenci 365 prostředí a bez nutnosti instalovat dodatečné externí komponenty. Požadujeme předložit link na dokumentaci popisující nastavení systému v jednotném grafickém rozhraní tak, aby získával logy z Office365/Mircosoft365.
		V případě krátkodobého (do 10 minut) až dvojnásobného přetížení systému proti jeho tabulkovým hodnotám nesmí dojít ke ztrátě logů nebo nesprávnému stanovení časového razítka. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti.
		Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno, zdrojová IP, značka/tag apod.).
		Dodavatel musí předložit potvrzení vystavené autorizovanou osobou o shodě, že nabízený systém splňuje požadavky normy ČSN/ISO 27001:2013 na pořizování auditních záznamů. Toto potvrzení není možné nahradit certifikátem na společnost dodavatele (subdodavatele) nebo výrobce nabízeného systému. Nelze nahradit čestným prohlášením.
		Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Továrně dodané pohledy na data nesmí jít administrátorem ani uživatelem systému nevratně modifikovat nebo smazat.
		Systém obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Pro vytváření nových pohledů na data není přípustné používat povinně SQL jazyk.
		Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.
		Na základě pohledu na uložená data lze provést export dat ve strukturovaném formátu tak, jak jsou v továrně nastaveném nebo uživatelsky nastaveném pohledu data skutečně zobrazena.
		Konfigurační a Systémové rozhraní a dokumentace k těmto rozhraním musí být identické v anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce nebo zjednodušená dokumentace odkazující na další dokumentaci v anglickém jazyce, případně na dokumentaci třetích stran. Požadujeme předložit link na online dokumentaci nebo připojit pdf aktuální kompletní dokumentace k ověření jednotlivých vlastností navrhovaného systému.
		Systém nabízí kapacitní i výkonovou škálovatelnost.
		Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 4TB.
		Požadujeme, aby systém obsahoval REST-API pro integraci s externím monitorovacím systémem (Zabbix, Nagios, MRTG a další) a umožňoval autorizovaný přístup ke strukturované databázi logů. Požadujeme předložit vzorový návod na integraci s externím monitorovacím systémem.
		Dodavatel doloží prohlášení výrobce o shodě s požadavky Vyhlášky 82 / 2018 Sb. „o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)“ k Zákonu 181 / 2014 Sb. „o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)“.
		Jednotná centrální webová konzole s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. Není přípustné, aby navrhovaný systém měl více rozdílných konzolí od různých výrobců s rozdílným ovládáním nebo aby se konfigurace musela provádět mimo jednotné webové rozhraní. Požadujeme předložit dokumentaci, ze které je zřejmé, jakým způsobem je realizována konfigurace v rámci jednotné konzole.
		Požadujeme, aby systém umožňoval jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem na základě typu zdrojů a značek a k jednotlivým ovládacím komponentům systému. Připojte odkaz na dokumentaci popisující vytváření uživatelských rolí v grafickém rozhraní systému.
		Dodaný systém musí obsahovat ucelené all-in-one řešení pro parsování a normalizaci přijatých událostí bez nutnosti dodatečné instalace externích aplikací nebo systémů. Jedinou přípustnou výjimkou je monitorování systémů Windows pomocí agentů.
		Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem.
	Kompatibilita	VMWare ESXi a Microsoft Hyper-V
	Podpora	Minimálně 60 měsíců včetně poskytnutí nových a opravných verzí

Komodita D – Server, diskové pole, UPS a zálohování		
Část	**Parametr**	**Popis povinného parametru**
D001	Provedení	RACK 19”, včetně výsuvných kolejnic, celková výška maximálně 2U, zaručený provoz při teplotě 30°C
	Procesor	2 sockety, osazen jeden CPU, každý právě 16 jader, min. základní frekvence 2,0 GHz, min. frekvence MEMBUS 4400 MHz, max. TDP 150W.

Server **1x**		Požadovaný výkon při osazení 2x CPU min.: - SPECrate2017_int_base min. 282 - SPECrate2017_fp_base min. 368 - Overall SPECpower_ssj2008 min. 14000 Požadujeme CPU poslední generace.
	Paměť	RAM min. 128 GB, 32 paměťových slotů, min. rozšiřitelnost až na 8 TB, osazeno 4x 32GB 2Rx8 DDR5-4800 Reg ECC
	Pevné disky	Min. 1x 240 GB SSD. Disk musí být hot-plug, server obsahuje dalších min. 7 volných funkčních 3,5" slotů pro disky.
	Porty	Min. 5x USB port v3.0 nebo vyšší: - min.2x přední - min 2x zadní, - min. 1x interní. Možnost osadit sériový port nezabírající PCIe slot.
	Chlazení	Redundantní hotswapové ventilátory
	LAN	min. jeden 1 Gbit RJ45 port nezabírající PCIe slot 4x 10 Gbps SFP+ 4x 1 Gpps TP
	PCI sloty	Volné PCIe sloty: - min. 1x PCI-Express 5.0 x8 a - min. 3x PCI-Express 5.0 x16
	Vzdálená správa	HW management, zapnutí, vypnutí, restart serveru, přesměrování KVM nezávislé na OS, vzdálené připojení médií. Interní management serveru umožňuje update serveru online z OS i offline bez nutnosti instalace dalšího nástroje pro správu, umožňuje bootu a instalace z interní SD karty o velikosti alespoň 16 GB. Dedikovaný LAN port pro management 1 Gbps RJ45. Možnost sdílení management portu s jiným Ethernet portem serveru. Časově neomezená licence.
	Napájení	2x redundantní napájecí zdroj min. 850 W každý, účinnost min. 96% Titanium, server musí běžet i při napájení pouze jednoho zdroje. Napájecí kabely min. 2,5 m. Spotřeba serveru v nabízené konfiguraci při 100% zatížení max. 360 W.
	Podpora operačních systémů a hypervizorů	Podpora nejrozšířenějších operačních systémů (Windows Server, Linux, VMware ESX) v nejnovější verzi
	Záruka	min. 60 měsíců poskytovaná **výrobcem v místě instalace** s reakcí nejpozději následující pracovní den po nahlášení závady
D002 **Diskové pole** **1x**	Provedení	Diskové pole s výškou max. 2U, včetně montážního materiálu do racku (ližiny pro rack), maximální montážní hloubka 500 mm.
	Pozice, rozšiřitelnost	minimálně 24 pozice pro HDD/SSD formátu 2,5", rozšiřitelnost minimálně na 48 disků.
	Spotřeba	Maximální spotřeba celé konfigurace při 100% zatížení 480 VA.
	Propustnost, latence	Minimální propustnost kontrolérů pole 100000 IOPS.
	Podporované typy disků	Podporované typy disků a jejich libovolné kombinace 3.5" Nearline SAS 22TB/18TB/12TB/8TB/4TB (7,200 rpm), 2,5" SSD 15,3TB/7,6TB/3,8TB/1,9TB/1,6TB, 2.5" SAS 1,8TB/1,2TB (10,000 rpm), možnost použití disků SED nebo FIPS.
	Podpora RAID technologií	Podpora typů RAID 0, 1, 1+0, 3, 5, 6, DDP s funkcí rychlého zotavení. Trvalá licence pro všechny uvedené typy RAID.
	Osazení disky	Minimální osazení disky: 6 kusů SAS 1,8TB 2,5" 10kRPM a 6 kusů disků SSD 1,9TB.
	Využitelná kapacita	Min. čistá využitelná kapacita pro připojené servery 8,5TB SAS (s nastavenou ochranou proti výpadku jednoho disku, např. RAID5) a 6,9TB SSD (s nastavenou ochranou proti výpadku jednoho disku, např. RAID5).
	Řadiče	2 redundantní řadiče iSCSI, každý s 2x SFP+ rozhraním s rychlostí 10 Gbps
	Kabely	2x DAC aktivní kabel 10Gb 5m.
	Vyrovnávací paměť (cache)	Minimální kapacita cache 16GB.
	Ochrana cache	Ochrana cache řadičů vůči výpadku napájení. V případě výpadku napájení musí být neuložená data zachována.
	Front-End porty	Minimální počet konfigurovatelných Front-End portů 8 na celé pole. Podporované typy Front-End portů FC 16 Gbps LC, iSCSI 1 Gbps RJ45, iSCSI 10 Gbps SFP.

	Přístup k managementu	Management porty LAN port 10/100/1000 Mbps min. 1 na každém řadiči. Bezpečný přístup k managementu pomocí protokolů SSL a SSH.
	Počet iSCSI portů	Minimální počet konfigurovaných iSCSI portů 10 Gbps SFP+ 4 ks.
	Správa diskového pole	SW pro kompletní vzdálenou správu pole + webové rozhraní, které umožní kompletní správu pole z libovoln0ho webového prohlížeče.
	Počet snapshotů	Minimální počet snapshotů a klonů 128.
	Licenční politika	Žádná dodaná licence nesmí být vázána na počet připojených serverů ani na kapacitu diskového pole ani na jednotlivé disky a pokud ano, tak musí pokrývat celkovou maximální rozšiřitelnost pole.
	SNMP, hlášení poruch	Podporované verze SNMP v2c, REST. Podpora zasílání alertů e-mail alert a trap, integrovatelné do nástrojů pro vzdálenou správu, požadujeme aktuální MIB soubor po každé aktualizaci fw.
	HOT-PLUG technplogie	Všechny komponenty pole musí být hot-plug, zejména řadiče, ventilátory, zdroje, IO moduly a pevné disky.
	Minimální počet připojených serverů	Minimální počet připojitelných serverů 128. Licence pro jejich připojení a MPIO musí být součástí nabídky.
	Provozní parametry	Rozsah provozních teplot 5-40°C, rozsah provozních vlhkostí 10-85%.
	Záruka	min. 60 měsíců poskytovaná **výrobcem v místě instalace** s garantovanou reakcí nejpozději následující pracovní den po nahlášení závady.
D003 **UPS pro server** **1 ks**	Provedení	UPS min. 2200VA, provedení do Racku, výška max. 2U, max. hloubka 70 cm
	Výstupní výkon	min. 1950W
	Doba provozu na baterie	Min. 45 minut při zátěži 400W, min. 28 min. při zátěži 600W
	Topologie	Line-interactive
	Výstupní přípojky	min. 8ks typu IEC 320 C13 (všechny umožňují provoz na baterie)
	Vstup	Jmenovité vstupní napětí [V]: 230 Kmitočet na vstupu [Hz]: 50/60 Hz +/- 3 Hz (autodetekce) Rozsah vstupního napětí pro napájení z rozvodné sítě: 160 – 286V
	Komunikace a správa	Port rozhraní: RJ-45 10/100 Base-T, RJ-45 Serial, SmartSlot, USB Ovládací panel: LED diody zobrazují stav – minimálně: - napájení ze sítě - napájení z baterie - vyměnit baterii - přetížení Zvukové upozornění: Upozornění na stav, kdy je systém napájen z baterie, zřetelné upozornění na nízkou kapacitu baterie
	Příslušenství	Hardware pro montáž do stojanu, skříňové podpěrné lišty, signalizační kabel, teplotní čidlo, kabel USB
	Softwarová podpora	Součástí dodávky bude software pro běžné typy virtualizačních platforem (VMWARE, Microsoft Hyper-V), který umožní podle nastavených parametrů řádné ukončení práce virtuálních serverů a následné fyzické vypnutí serveru. Trvalá licence.
	Záruka	Minimálně 36 měsíců
D004 **Zálohovací zařízení** **1 ks**	Provedení	Samostatně stojící, možno umístit i mimo rack
	Pozice pro disky	Min. 8 pozic pro HDD / SSD, podpora Btrfs a ext4 souborových systémů, min. 1x PCIe Gen3 x2 slot pro rozšiřující kartu
	Operační paměť	Min. 8 GB DDR4 RAM
	Rozšiřitelnost	Podpora připojení externích disků přes USB 3.0 (min. 2 porty) + min. 1x eSATA port 2 x M.2 NVMe 2280 SSD slot pro SSD cache
	Výkon	Přenosová rychlost až 2300MB/s při osazení 10Gb LAN, IOPS při náhodném čtení 4K až 110 000
	Komunikace LAN	Síťové protokoly CIFS, WebDAV, iSCSI, SSH, SNMP, http/s
	Hot-swap	Disky vyměnitelné za chodu
	Kapacita	Osazeno min. 6ks 12TB HDD SATAIII/7200 RPM/256MB cache. Disky se zárukou 60 měsíců, uvedené v seznamu kompatibilních disků výrobce zálohovacího zařízení, automatická aktualizace firmware společně s aktualizacemi operačního systému zálohovacího zařízení.
	Konektivita	Min. 4x 1GBit Ethernet porty s podporou agregace linek a redundance. Min. 2x 10Gbit SFP+ porty
	Disková cache	Osazeny 2 ks SSD M.2 NVMe modulů s kapacitou min. 400 GB (cache pro čtení i zápis)

	Ochrana dat	Basic/JBOD/0/1/5/5+Spare/6/10 + Hybrid RAID
	Podpora	Podpora virtualizace a iSCSI (VMware vSphere® 6,5, Microsoft Hyper-V®, Citrix®, OpenStack®), podpora Windows ADS, podpora AES 256bit šifrování svazku
	Software	Zařízení musí obsahovat časově neomezené služby pro zálohování pracovních stanic, pro zálohování jiných zařízení NAS, pro zálohování fyzických i virtuálních serverů a pro zálohování Microsoft 365 a G-Suite.
	Podpora UPS	Podpora korektního vypnutí signálem z UPS přes LAN při výpadku napájení
	Záruka	Minimálně 36 měsíců
D005 **UPS pro zálohovací zařízení** **1 ks**	Provedení	Volně stojící
	Příkon	Min. 1200VA
	Výkon	Min. 650W
	Zásuvky	České zásuvky, minimálně 4 ks
	Komunikace	USB port
	Záruka	Min. 24 měsíců
SW pro virtualizaci	Využití licence zadavatele	Pro instalaci virtuálních serverů bude použit hypervizor VMWARE vSphere 8 Essentials kit - zadavatel má zakoupenou trvalou licenci s podporou do 31. ledna 2027.
D006 **SW licence zálohovací software** **1ks**	Licence	Licence zálohovacího software pro min. 10 zálohovaných zařízení (nerozlišuje se mezi VM, fyzickýcm serverem, PC - univerzální použití licence) bez omezení objemu dat
	Efektivita ukládání dat	Integrovaná technologie komprimace a deduplikace.
	Nároky na správu	„Bezagentové" řešení – není nutná instalace agentů do zálohovaných virtuálních serverů nebo aplikací. Možnost replikace virtuálních strojů na jiný virtualizační nod za chodu serveru
	Ochrana dat	Provádění datově konzistentních záloh hlavních serverových aplikací - MS SQL, Active Directory, souborové systémy - bez nutnosti odstávky aplikace
	Fyzické servery	Vestavěná podpora zálohování fyzických serverů - pro fyzické servery je přípustné využívat agenty. Podpora ukládání záloh nevirtualizovaných serverů a PC do společného úložiště a monitorování zálohovacích úloh.
	Snapshoty	Využívání snapshotů, zálohování pouze dat změněných od poslední úspěšné zálohy. Podpora operačních systémů Windows a Linux v zálohovaných virtuálních serverech.
	Ověření záloh	Možnost otestování a ověření každého zálohovaného VM a jeho obnovitelnosti spuštěním přímo ze souboru zálohy; včetně podpory pro vlastní testovací skripty.
	Obnova položek Active Directory	Obnova jednotlivých objektů i skupin objektů Active Directory – uživatelů, skupin, kontejnerů, objektů Group Policy včetně hromadného výběru a obnovy hesel účtů
	Uložiště záloh	Možnost ukládání záloh na diskový prostor. Možnost nouzového spuštění zazálohovaného virtuálního serveru z NAS v izolovaném prostředí bez nutnosti obnovy
	Správa	Vytváření a správa úloh (zálohování, obnova apod.) pomocí průvodců. Automatický reporting úspěšných i neúspěšných úloh. Běžné úlohy obnovy (obnovení souboru, databáze SQL, objekty Active Directory) provádět pomocí průvodců.
	Záruka a nárok na nové verze	Záruka 60 měsíců včetně nároku na nové verze software.
D007 **Rack pro server**	Provedeni	Rack 42U pro umístění serveru, diskového pole a UPS, šířka 800 mm, hloubka 1200 mm, přední i zadní dveře perforované
	Police	2x Police 1U/750mm, s nosností až 80 kg
	Chlazení	Ventilátorová jednotka vrchní včetně termostatu

Komodita E – Koncová zařízení		
Část	**Parametr**	**Popis povinného parametru**
E001 **Notebook** **22 ks**	Displej	Úhlopříčka min. 16", poměr stran 16:10, rozlišení min. 1920 x 1200 bodů
	CPU	CPU s bodovým hodnocením min. 16 000 bodů dle https://www.cpubenchmark.net/
	RAM	Min. 16 GB
	Disk	Podpora PCIe® 4.0x4 NVMe®, osazený 1 ks SSD disk s kapacitou min. 500 GB + možnost doplnit další SSD s kapacitou až 2 TB
	Připojení	Bluetooth verze min. 5.1, WIFI standardu 6, Ethernet 10/100 Mbit/s
	Kamera	Kamera s FHD rozlišením a s krytkou

	Porty	1x Ethernet (RJ-45) 1x HDMI® 2.1, až 4K/60Hz 1x kombinovaný konektor pro sluchátka / mikrofon (3,5 mm) 1x čtečka SD karet 1x Thunderbolt™ 4 / USB4® 40 Gbps (podpora přenosu dat, Power Delivery 3.0 a DisplayPort™ 1.4) 1x USB 3.2 Gen 1 1x USB 3.2 Gen 1 (vždy zapnuto) 1x USB-C® 3.2 Gen 2 (podpora přenosu dat, Power Delivery 3.0 a DisplayPort™ 1.4)
	Klávesnice	Podsvícená klávesnice s CZ/SK popisy a s numerickou částí
	Zvuk	Stereo reproduktory, 2W x 2, Dolby® Audio™, 2x mikrofon
	Zabezpečení	Firmware TPM 2.0 , snímač otisků prstů, IR kamera pro Windows® Hello
	Baterie	Min. 45 Wh
	Napájecí adaptér	Min. 65W, napájení notebooku přes USB-C port
	Mechanická odolnost	Kovový horní kryt (například hliník)
	Certifikace	ENERGY STAR® 8.0, certifikace TCO 9.0, soulad s RoHS
	Certifikace odolnosti	Vojenský test MIL-STD-810H
	Operační systém	WINDOWS verze PRO v nejnovější dostupné verzi (nutné pro zajištění 100% kompatibility s provozovanými aplikacemi)
	Záruka	Min. 36 měsíců poskytovaná výrobcem s opravou v místě instalace (on-site)
E002 **Dokovací stanice pro notebook** **21 ks**	Popis	Dokovací stanice USB-C 100% kompatibilní s dodanými notebooky
	Video porty	Min. 2x DP, 1x HDMI
	USB porty	Min. 3x USB 3.1, 2x USB 2.0, 1x USB-C
	Audio porty	1x Combo 3,5 mm audio Jack
	Ethernet	Min. 1x Gigabit Ethernet
	Power Delivery	Min. 65W s 90W napájecím adaptérem (součást dodávky)
	Záruka	Min. 36 měsíců
E003 **Projektor včetně držáku a montáže** **17 ks**	Popis	Projektor do učeben s možností montáže na strop
	Rozlišení	1920x1080 bodů, poměr stran 16:9
	Svítivost [lm]	Min. 4000
	Kontrast	Min. 16000:1
	Životnost lampy [h]	Min. 6500 v běžném režimu, 17000 (v úsporném režimu
	Rozhraní – minimálně	- USB 2.0 Type A - USB 2.0 Type B - RS-232C - Wired Network - VGA in (2x) - VGA out - HDMI in (2x) - Composite in - Stereo mini jack audio out - Stereo mini jack audio in (2x) - Cinch audio out - Microphone input - Wireless LAN IEEE 802.11b/g/n - Miracast
	Další požadavky	Dodávka včetně stropního držáku a potřebných propojovacích kabelů

5 Požadavky na instalační a implementační práce

Součástí dodávky technologií bude jejich dodávka, instalace a implementace do prostředí kupujícího s jejich konfigurací v rozsahu tak, aby došlo k naplnění požadavků standardu konektivity uvedeného v tabulce níže. Veškeré možné související dodávky a služby, které plynou z tabulky uvedené níže prodávající musí zohlednit ve svém plnění a dodat tak, aby došlo k plnění požadovaných parametrů konektivity definovaných v této tabulce.
Součástí předmětu plnění jsou dále i služby a práce prodávajícího se zařízeními a licencemi přímo související a nezbytné k řádnému uvedení předmětu plnění do provozu:

- Provedení předimplementační analýzy (včetně plánovaných změn v konfiguraci současné infrastruktury) a zpracování detailního finálního popisu cílového stavu a postupu implementace.
- Zpracování prováděcí dokumentace, podle které bude dodavatel řešení implementovat. Prováděcí dokumentace musí být před zahájením implementace výslovně schválena zadavatelem. Prováděcí dokumentace musí vycházet z předimplementační analýzy a respektovat a využívat osvědčené praktiky (tzv. Best Practices) a doporučení výrobců nabízených technologií.
- Dodávka a implementace předmětu plnění dle schválené prováděcí dokumentace včetně technické podpory.
- Zajištění projektového vedení realizace předmětu plnění.
- 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
  - 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 10 a vyšších, Android, iOS a MacOS.
- Zpracování dokumentu Zásady využívání ICT a přístupu k síti dle Standardu konektivity pro začlenění do vnitřních předpisů školy.
- Zpracování materiálů pro školení a provedení školení.
- Zajištění zkušebního provozu infrastruktury v délce minimálně 2 týdnů včetně technické podpory specialistů na dané zařízení/službu s dostupností maximálně do 2 hodin na místě realizace od nahlášení požadavku v pracovní den v době od 8h do 17h.
- zpracování a předání instalační dokumentace,
- zpracování a předání administrátorské dokumentace
- Provedení akceptačních testů.
- Předání do plného provozu.

Požadujeme, aby práce mající dopad do fungování IT prostředí kupujícího, byly prováděny výhradně mimo dobu výuky (tedy byly prováděny v časech 16:00 – 6:00, případně mimo pracovní dny kdykoliv). Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standartních formátech (např. MS Office) používaných kupujícím na datovém nosiči a 1x kopii v papírové formě.

5.1 Instalační a implementační služby v oblasti sítě

Po dokončení plnění dle této specifikace bude škola plně pokryta LAN i WiFi sítěmi s parametry vyhovujícími technickým požadavkům Standardu konektivity. Školní síť bude podporovat IPV6, bude

chráněna Firewallem a provoz na síti bude monitorován a logován. Přístup do sítě bude zabezpečen protokolem 802.1X. Jedná se zejména o následující:

- Bude implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby s využitím technologie 802.1x.
- 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.
- 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).
- Architektura WiFi bude založena na řešení s centrální správou prováděnou hardwarovým, SW, nebo virtuálním kontrolérem (řadičem). Kontrolér 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.
- Ověřování přístupu do LAN bude realizováno protokolem 802.1x vůči adresářové službě prostřednictvím protokolů radius a P/EAP. Používaná zařízení (min. stolní i přenosné počítače) budou vybavena tzv. suplikantem-softwarovou komponentou, která dokáže předávat ověřovací požadavky síťovým prvkům, které tyto požadavky ověří vůči adresářové službě. 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.
- 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 radius servery. Učitelé a žáci budou prostřednictvím radius serveru ověřováni v adresářové služby. Zabezpečení vnitřních sítí (BSSID) školy bude provedeno dle 802.1i, tedy-WPA3 (v odůvodněných případech 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 nebo jiné technologie s tzv. lobby přístupem pro správu a generování účtů/kupónů ne-technickou osobou.
- Federovaný systém EDUROAM (www.eduroam.cz) umožňuje přistupovat k sítím subjektů zapojených v systému a prostřednictvím těchto sítí k dalším službám, typicky internetu. Federace umožňuje ověření uživatele v libovolné zapojené síti (v České republice i zahraničí) pomocí uživatelovy jediné (centrální) identity. Správcem systému EDU je společnost Cesnet. V rámci projektu bude realizováno připojení do systému EDUROAM a bude nakonfigurováno

připojení WiFi sítě do systému EDUROM prostřednictvím vybudované autentizační a autorizační platformy na bázi radius serverů a adresářové služby. Současně budou realizovány další netechnické požadavky pro provoz EDUROAM – zejména vytvoření informační webové stránky a zajištění technického kontaktu. Zapojení do systému EDUROAM umožní národní i mezinárodní mobilitu žáků a učitelů.

V rámci výše uvedeného nasazení technologií budou provedeny minimálně následující služby:

- Analýza stávajícího síťového prostředí a návrh nového architektury LAN i WiFi
- Implementace pořízených technologií
- Provedení segmentace LAN – VLAN, adresování, směrování/routování
- Zavedení IPv6 pro přístup k internetovým zdrojům publikovaným na IPv6 adresách
- Zavedení IPv6 pro veškeré publikované služby z interních či externích prostředků. Včetně součinnosti pro zajištění změn u externích poskytovatelů služeb. Jde zejména (ale ne výhradně) o služby hostování domén škol, DNS, e-mail, weby škol, publikované nebo hostované školské informační systémy.
- Zavedení DNSSEC pro interní DNS služby i součinnost při zabezpečení domén škol. Dodavatel poskytne škole písemně parametry nutné pro správnou konfiguraci DNSSEC u poskytovatele internetového připojení. Škola zajistí nutnou součinnost pro správné nastavení parametrů DNSSEC.
- 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
- Návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) pro školy
- Vybudování VPN pro vzdálený přístup uživatelů LAN na bázi webového portálu s využitím dodaných technologií.
- Návrh a provedení akceptačních testů, musí zahrnovat testy propustnosti LAN a pokrytí WiFi

5.2 Instalační a implementační služby v oblasti centrálního logování

Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací. 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).
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.
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.
Z pohledu požadavku 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. 3 měsíce. Na tento rozsah retence musí být systém dostatečně

dimenzován, tak aby nedocházelo k výkonovým problémům a systém měl dostatečnou rezervu pro očekávatelný budoucí nárůst informací a jejich zdrojů.
Technicky se může jednat o virtuální appliance nebo o samostatné komplexní řešení. V případě, že bude použito virtuální řešení nainstalované na centrálním serveru, nesmí systém centrálního logování při plné zátěži spotřebovat více než 30% systémových zdrojů centrálního serveru.
V rámci výše uvedeného nasazení technologií budou provedeny minimálně následující služby:

- 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.)
- Provedení souvisejících konfigurací monitorovaných systémů (vyplývá z požadavků standardu konektivity)
- Návrh a provedení akceptačních testů, musí zahrnovat ověření logování veškerých požadovaných uživatelů a správnost přiřazení identit uživatelů logovaným údajům

5.3 Instalační a implementační služby v oblasti serveru, zálohování data a energie a serverových operačních systémů

V rámci plnění bude nasazen nový server, který bude sloužit jako hlavní virtualizační platforma, a to jak pro nově pořízené technologie, tak pro současné. Server bude připojen optickou linkou 4x 10Gbit/s do páteřní sítě školy. Dodávka nových licencí operačních systémů a klientské přístupové licence jsou také součástí plnění.
Prodávající provede přesun virtuálních serverů a služeb ze stávajícího na nový server v rámci stejné virtualizační platformy a bude také proveden upgrade všech operačních systémů na nejnovější dostupné verze.
Bude nasazena ochranou nově pořízených technologií vůči výpadku elektrického proudu v podobě UPS
Dodávka licencí pro hypervizor není součástí projektu – bude použita technologie Hyper-V, která bude součástí dodávaného serverového operačního systému.
Aktuálně používaný systém zálohování bude nahrazen novým síťovým úložištěm „NAS" s dostatečnou kapacitou pro ukládání provozních záloh. Zálohování bude řízeno pokročilým zálohovacím softwarem, který bude prostřednictvím virtualizačního hypervizoru zálohovat všechny virtuální servery. Zálohovací systém umožní zálohovat i fyzické servery a osobní počítače. Síťové úložiště NAS bude kvůli bezpečnému oddělení záloh umístěno mimo místnost serveru.
Licence operačních systémů musí umožnit využití implementovaných funkcionalit serverových řešení. Požadované licence desktopových operačních systémů musí umožnit začlenění stávajících počítačů pod kontrolu a centrální řízení adresářové služby Active Directory, ověřování přístupu k síti a poskytování potřebných informací pro systém centrálního logování.
Pro obvyklá zařízení využívané školami a určená k připojení do počítačové sítě (kategorie stolní a přenosné počítače, tiskárny, tablety a chytré telefony, ostatní síťová koncová zařízení) bude předvedena vzorová konfigurace a plné funkcionalita zařízení v síti, dále bude provedeno seznámení s vazbami zabezpečení sítě-konfigurace zařízení a demonstrováno logování provozu zařízení a činnosti jeho uživatele. Předvedení bude provedeno pro takový počet vzorků, aby byly pokryty významné odlišnosti vzorků v rámci kategorie z pohledu funkcí či potřebných konfigurací (např. tablety s OS Android a IOS).

5.4 Instalační a implementační služby v oblasti koncových zařízení

Součástí komodity je dodávka, instalace a konfigurace koncových zařízení potřebných pro vedení výuky.
U PC se bude jednat zejména o jejich zapojení a napojení na MS Active Directory
U projektorů se bude jednat o jejich montáž, napojení na zdroje signálu a dat, předvedení a ověření funkčnosti.

5.5 Školení

Prodávající provede pro každý typ zařízení a software odborné školení na obsluhu a práci s dodanými zařízeními, a to minimálně v rozsahu provozní dokumentace.
Školení bude pokrývat všechna zařízení a systémy všech komodit, dodávané v rámci plnění této specifikace, a to minimálně v rozsahu:

- běžných administrátorských činností pro implementované systémy
- standardní údržby systémů pro administrátory zadavatele

Školení dále zajistí seznámení pracovníků zadavatele se všemi podstatnými částmi plnění v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.
Minimální rozsah školení pro každé zařízení a software jsou 2 hodiny, není-li uvedeno jinak. Školení bude probíhat v sídle kupujícího. Počet školených osob kupujícího je stanovena na max. 3 osoby.

5.6 Plnění standardu konektivity škol

Předmět plnění dle této technické specifikace slouží k naplnění účelu dosažení standardu konektivity školy stanovenému na URL: https://www.edu.cz/digitalizujeme/standard-konektivity-skol/
Prodávajícího se v rámci realizace tohoto plnění zavazuje pro kupujícího dodat a nakonfigurovat technologie tak, aby jejich prostřednictvím bylo dosaženo standardu konektivity, a to v rozsahu, ve kterém jsou tyto technologie pro plnění standardu konektivity pořizovány.

Dále se prodávající zavazuje poskytnout kupujícímu součinnost a zejména konkrétní sestavení požadavků na plnění standardu konektivity z pohledu služeb **poskytovatele internetového připojení** tak, aby v návaznosti na nasazené technologie bylo možné u poskytovatele internetového připojení provést zbývající konfigurace k dosažení potřebného naplnění standardu konektivity dostupnému na výše uvedeném URL. Prodávající za tímto účelem poskytne kupujícímu až 5 hodin odborných konzultačních služeb, jejichž součástí bude písemné zpracování požadavků na změnu služeb a technologií na straně poskytovatele internetového připojení a dále konzultace k jejich nasazení.

Dále se prodávající zavazuje poskytnout kupujícímu součinnost a zejména konkrétní sestavení požadavků na plnění standardu konektivity z pohledu služeb **poskytovatele hostingu** webových stránek a emailů školy tak, by tyto služby byly zabezpečeny v rozsahu definovaném standardem konektivity, tedy zejména DNSSEC. Prodávající za tímto účelem poskytne kupujícímu až 5 hodin odborných konzultačních služeb, jejichž součástí bude písemné zpracování požadavků na změnu služeb a technologií na straně poskytovatele hostingu a dále konzultace k jejich nasazení.

Prodávající je dále povinen v rámci plnění standardu konektivity dostupném na výše uvedeném URL pro kupujícího navrhnout **Směrnici a další dokumentaci**, kterou standard konektivity vyžaduje a je ji potřeba předložit k prokázání jeho dosažení. Směrnice musí odpovídat minimálnímu rozsahu stanovenému standardem konektivity, zohledňovat nasazené technologie a zajistit synergii procesů stanovených touto směrnicí s nově vybudovaným a vybaveným technologickým prostředím školy.

Veškerou součinnost poskytovatele internetového připojení kupujícího zajišťuje kupující. Pro podání nabídky proto služby poskytovatele internetového připojení nevstupují jako součást plnění a není proto ze strany prodávajícího potřeba zajistit pro jeho nabídku potřebou přímou součinnost poskytovatele internetového připojení kupujícího.

V rámci plnění této specifikace nedochází k budování ICT kabelových rozvodů, které jsou samostatným plnění mimo plnění podle této dokumentace. ICT kabelové rozvody budou vybudovány a připraveny pro realizaci tohoto plnění.

Plnění Standardu konektivity škol, kterého musí být v rámci realizace plnění dle této specifikace dosaženo je mimo jiné definované v následující podobě (uvedeno ve sloupci komentář), které kupující užil jako stanovení cíle pro dotační žádost, ze které bude toto plnění kofinancováno:

Parametr	**Plnění (ano/ne/ nerelevantní)**	**Komentář**
Konektivita školy k veřejnému internetu (WAN) - povinné parametry		
Šíře pásma (bandwidth) odpovídající 0,25 Mbps/žák či student nebo 0,5 Mbps/koncové uživatelské zařízení a zároveň taková šířka pásma, která neomezuje provoz zařízení a uživatelů. Šíře pásma se vztahuje na počet žáků/studentů/koncových uživatelských zařízení v budově/areálu, kde se projekt realizuje	Ano	Tento parametr škola v současné době splňuje.
Vlastní nebo poskytovatelem přidělené veřejné IPv4 adresy.	Ano	Tento parametr škola v současné době splňuje.
Zajištění monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu koncovému zařízení v minimální délce 3 měsíců.	Ano	Tento parametr škola v současné době nesplňuje, proto bude v rámci projektu implementován systém "log management". Tím bude parametr naplněn.
Síťové zařízení podporující rate limiting, antispoofing, access listy - zařízení musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality.	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní síťové prvky (firewall, přepínače, WiFi AP) s požadovanými funkcemi. Tím bude parametr naplněn.
Schopnost snadné/automatické rekonfigurace pravidel firewallu (access listů) na základě identifikovaných útoků.	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní síťové prvky (firewall, přepínače, WiFi AP) s požadovanými funkcemi. Tím bude parametr naplněn.
Zajištění šifrovaného přístupu (SSL/TLS) a podepsání DNSSEC domén pro služby školy dostupné online (např. emailové služby, webové servery, studijní a ekonomické agendy atp.).	Ano	Tento parametr škola v současné době nesplňuje, proto bude v rámci projektu pořízen wildcard certifikát a bude provedena rozšířená konfigurace DNS serveru. Tím bude parametr naplněn.
Validující DNSSEC resolver na straně školy, nebo poskytovatele konektivity, nebo otevřeným DNSSEC validujícím resolverem	Ano	Tento parametr škola v současné době nesplňuje, proto bude v rámci projektu provedena rozšířená konfigurace DNS serveru. Tím bude parametr naplněn.

Software a firmware je aktualizován po dobu udržitelnosti projektu, jsou-li aktualizace k dispozici	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní síťové prvky (firewall, přepínače, WiFi AP) s požadovanými funkcemi. Tím bude parametr naplněn.
Poskytovatel konektivity je schopen zajistit kontaktní bod pro komunikaci, trvalý monitoring dostupnosti konektivity, realizovat blokování nežádoucí komunikace zahlcující nebo jinak omezující konektivitu a systémy školy na straně poskytovatele na základě požadavku školy.	Ano	Tento parametr škola v současné době splňuje
Konektivita školy k veřejnému internetu (WAN) - doporučené parametry		
Symetrické připojení (zajištění konektivity) bez agregace a omezení.	Ano	Tento parametr škola v současné době splňuje.
Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6, včetně zajištění dostupnosti online služeb školy na IPv6 adresách.	Ano	Tento parametr škola v současné době nesplňuje. Budou pořízeny aktivní prvky s podporou IPv6 a ve spolupráci s poskytovatelem internetu provedena konfigurace, tím bude parametr naplněn.
Poskytovatel konektivity je schopen zajistit funkci systému incident response, monitoring a aktivní notifikaci anomálií síťového provozu, zamezení podvržení zdrojových IP adres (anti-spoofing), funkci pro blokování nežádoucí komunikace zahlcující nebo jinak omezující konektivitu a systémy školy pro zamezení zahlcení linky (např. RTBH, FlowSpec, služby AntiDDoS řešení), detekci a zamezení amplifikačních útoků, zabezpečení směrování síťového provozu pomocí RPKI a konfigurace odmítnutí nevalidních prefixů.	Nerelevantní pro tento projekt	
Antivirová kontrola internetového provozu	Nerelevantní pro tento projekt	
Vnitřní konektivita školy (LAN a WLAN) - společné povinné parametry		
Systém správy uživatelů (Identity Management), tj. centrální databáze identit (LDAP, AD apod.) a její využití pro autentizaci uživatelů (žáci i učitelé) za účelem bezpečného a auditovatelného přístupu k síti, resp. službám. Využívání jednoho účtu více uživateli není povoleno (využívání tzv. anonymních účtů).	Ano	Tento parametr škola v současné době nesplňuje. Budou pořízeny aktivní prvky , server a serverový OS s podporou auditovatelného přístupu k síti a tím bude parametr naplněn.
Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém	Ano	Tento parametr škola v současné době nesplňuje, proto bude v rámci projektu implementován systém "log management". Tím bude parametr naplněn.

Systémy zálohování a obnovy dat serverové infrastruktury	Ano	Tento parametr škola v současné době nesplňuje, proto bude v rámci projektu pořízen zálohovací SW a NAS a tím bude parametr naplněn.
Systémy pro antivirovou ochranu počítačových systémů, antispamovou ochranu poštovních serverů	Ano	Tento parametr škola v současné době splňuje.
Vnitřní konektivita školy (LAN a WLAN) - povinné parametry pevné LAN		
Minimální konektivita koncových uživatelských zařízení 1000 Mbps fullduplex	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní prvky a natažena kabeláž, tím bude parametr naplněn.
Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení (např. IPS, IDS, Next Generation Firewall aj.), datových úložišť (NAS) 1000 Mbps fullduplex	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní prvky a natažena kabeláž, tím bude parametr naplněn.
Síťové prvky musí splňovat následující funkcionality: centrální směrovače a centrální přepínače (L2 i L3) s neblokující architekturou přepínacího subsystému (wire speed), management, podpora 802.1Q VLAN (možnost tvorby virtuálních sítí - VLAN), základní bezpečnostní prvky proti zneužití přístupu k síti [např. MAC based omezení (port-sec), 802.1X autentizace aj.].	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní prvky a natažena kabeláž, tím bude parametr naplněn.
Strukturovaná kabeláž pro připojení počítačových systémů a dalších zařízení (tiskárny, servery, AP aj.).	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní prvky a natažena kabeláž, tím bude parametr naplněn.
Páteřní rozvody mezi budovami v areálu, kde probíhá výuka nebo příprava na ni, realizovány prostřednictvím optických vláken nebo metalických kabelů. Vztahuje se na budovu/areál, kde se projekt realizuje.	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní prvky a natažena kabeláž, tím bude parametr naplněn.
Vnitřní konektivita školy (LAN a WLAN) - povinné parametry bezdrátové sítě WLAN		
Návrh topologie Wi-Fi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů.	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní prvky, natažena kabeláž a nainstalovány WiFi vysílače, tím bude parametr naplněn.
Zabezpečení minimálně AES šifrováním a standardem WPA2-Enterprise nebo WPA3-Enterprise, multi SSID, ACL pro filtrování provozu.	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní prvky, natažena kabeláž a nainstalovány WiFi vysílače, tím bude parametr naplněn.

Zajištění vzájemně oddělených sítí pro zaměstnance školy, žáky/studenty školy a externí zařízení (hosty).	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní síťové prvky (WiFi AP) s požadovanými funkcemi. V rámci nové WiFi sítě budou zřízené nové SSID sítě, které oddělí zaměstnance školy, žáky/studenty školy a externí zařízení (hosty).
Podpora mechanismu izolace uživatelů.	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní síťové prvky (WiFi AP) s požadovanými funkcemi. Tím bude parametr naplněn.
Podpora standardu IEEE 802.11ac (Wi-Fi 5) a případně novějších (Wi-Fi 6), současná funkce AP v pásmu 2,4 a 5 GHz a novějších protokolů a pásem.	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní síťové prvky (WiFi AP s podporou Wi-Fi 6) s požadovanými funkcemi. Tím bude parametr naplněn.
Vnitřní konektivita školy (LAN a WLAN) - společné doporučené parametry		
Logování provozu za účelem dohledatelnosti na úroveň koncového uživatele.	Ano	Tento parametr škola v současné době nesplňuje. Budou pořízeny aktivní prvky, server a serverový OS s podporou auditovatelného přístupu k síti, implementován systém "log management". Tím bude parametr naplněn.
Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty) a systému blokace Wi-Fi v určitém čase.	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní síťové prvky (WiFi AP) s požadovanými funkcemi. Řešení bude vybudováno na Captive portálu. Tím bude parametr naplněn.
Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací (např. aktivní zapojení do federovaného systému www.eduroam.cz).	Ano	Tento parametr škola v současné době nesplňuje, bude implementován systém EDUROAM.
Centralizovaná architektura správy Wi-Fi sítě (centrální řadič, centrální management, tzv. thin access pointy, popř. alespoň centrální řešení distribuce konfigurací s podporou automatického rozložení zátěže klientů, roamingu mezi spravované access pointy a automatickým laděním kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení).	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní síťové prvky (WiFi AP) s požadovanými funkcemi. Tím bude parametr naplněn.
Doporučená podpora pro ověřování uživatelů oproti databázi účtů [např. pomocí protokolu IEEE 802.1X vůči centrální evidenci uživatelů (např. LDAP, MS AD) nebo pomocí Captive portalu].	Ano	Tento parametr škola v současné době nesplňuje. Nově pořízené technologie (switche, Wi-Fi AP) škole umožní vybudování RAIDUS serveru a captive portálu. Tím bude parametr naplněn.

Propojení aktivních prvků a důležitých systémů (např. Servery, NAS, propojení budov) rychlostí 10 Gbps, včetně uplinku.	Ano	Tento parametr škola v současné době nesplňuje, projekt počítá s pořízením všech klíčových zařízení s možností připojení 10Gbit. Tím bude parametr naplněn.
Doporučené bezpečnostní prvky projektu		
Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3917 - IPFIX nebo ekvivalent)	Nerelevantní pro tento projekt	
Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie.	Ano	Tento parametr škola v současné době nesplňuje. Budou pořízeny aktivní prvky, server a serverový OS s podporou auditovatelného přístupu k síti, implementován systém "log management", firewall Next generation. Tím bude parametr naplněn.
Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management).	Ano	Tento parametr škola v současné době nesplňuje, proto bude v rámci projektu implementován systém "log management". Tím bude parametr naplněn.
Systémy pro monitorování funkčnosti síťové a serverové infrastruktury.	Nerelevantní pro tento projekt	
Zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu.	Ano	Tento parametr škola v současné době nesplňuje. Budou pořízeny aktivní prvky s požadovanou funkcionalitou, tím bude parametr naplněn.
Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk aj.).	Nerelevantní pro tento projekt	
Nástroje pro centrální správu a audit ICT prostředků.	Nerelevantní pro tento projekt	
Podpora vzdáleného přístupu (VPN).	Ano	Tento parametr škola v současné době nesplňuje. Budou pořízeny aktivní prvky s požadovanou funkcionalitou, tím bude parametr naplněn.
Zavedení více-faktorové autentizace.	Nerelevantní pro tento projekt	

Povinným akceptačním kritériem bude prokázání naplnění požadavků Standardu konektivity škol dle manuálu uveřejněného na Standard konektivity a bezpečnosti škol - edu.cz včetně úspěšného provedení a doložení testu na https://www.standardkonektivity.cz/. Prokázání naplnění požadavků poskytne prodávající v písemné formě vhodné jako přílohu k Závěrečné zprávě o realizaci projektu.

Kupující upozorňuje, že pro dosažení naplnění standardu konektivity jsou potřeby i služby poskytovatele internetového připojení a hostingu kupující, pro něž prodávající písemně poskytne potřebné požadavky na konfigurace. Prodávající proto v rámci svého plnění musí postupovat tak, aby tyto třetí strany měli odpovídající časový prostor v rámci jejich součinnosti zajišťované kupujícím tyto

konfigurace nastavit a prodávající pak mohl jako pro kupujícího zajistit komplexní výstupy naplnění standardu konektivity, které následně kupujícímu poslouží jako výstup pro prokázání naplnění požadavků jím realizovaným projektem.

6 Záruky a servisní podmínky

6.1 Požadavky na záruky a servisní podmínky

(1) Zadavatel uvádí u jednotlivých komodit, resp. jejich částí požadovanou min. záruku, popř. podporu. Uváděné parametry byly průzkumem trhu zjištěny jako standardní, tj. poskytovány výrobci jako součást standardní dodávky a ceny. Není-li záruka části uvedena, je pro tuto část požadována záruka min. 24 měsíců.

(2) Zadavatel požaduje bezplatný (zahrnutý v ceně zakázky) přístup k aktualizacím software a firmware dodaných komodit minimálně po dobu záruky.

(3) Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro zadavatele.

(4) Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.

(5) Není-li uvedeno u konkrétní komodity jinak, požaduje zadavatel provedení záruční opravy do pěti pracovních dnů.

(6) Po dobu 60 měsíců od předání díla jako celku do plného provozu, musí dodavatel nebo výrobce všech zařízení garantovat běžnou dostupnost náhradních komponentů a dostupnost servisu.

(7) Dodavatel ve své nabídce výslovně uvede všechny podmínky záruk.

6.2 Požadavky na zabezpečení provozu

(1) Z důvodu zajištění udržitelnosti projektu po dobu 60 měsíců a zajištění bezpečnosti provozu požaduje zadavatel zajištění poskytnutí podpory softwarových produktů.

(2) Podpora je požadována minimálně v rozsahu potřebném pro zajištění bezpečného provozu dodaných systémů.

(3) V případě požadavku zadavatele je uchazeč povinen podporu v tomto rozsahu poskytnout. Cenu poskytnutí uvede dodavatel v Příloze č. 1 Kupní smlouvy – Kalkulace nabídkové ceny do určených polí v listu Provoz.