Technická specifikace poptávaného plnění k veřejné zakázce „Konektivita – Gymnázium Ostrov“

OBSAH DOKUMENTACE

Popis výchozího stavu

Toto je popis stávajícího stavu IT infrastruktury GO. Jedná se o Gymnázium Ostrov, příspěvkovou organizaci, IČ: 49753771, na adrese Studentská 1205, 363 01 Ostrov, okres Karlovy Vary, Karlovarský kraj, Česká republika. Jde o státní školu, poskytující úplné střední vzdělání s maturitou, zařazené do sítě škol MŠMT, pro účely této zprávy dále označované jako „škola“ nebo „gymnázium“.

Současný stav ICT školy **neodpovídá Standardu konektivity škol** ani současným nárokům na výkon, bezpečnost a centralizovanou správu počítačové sítě. Počítačová síť byla budována postupně, stáří a technická úroveň používaných prvků se liší. Převážně jde o prvky technicky i morálně zastaralé a jejich výrobci již nepodporované. Chybí užší provázanost jednotlivých částí.

Absence možnosti centralizovaného detailního řízení a sledování provozu je klíčovou překážkou ve zvýšení úrovně kybernetické bezpečnosti a realizaci preventivních opatření. Decentralizovaná, resp. roztříštěná správa sítě bez podpůrných a automatizačních nástrojů vyčerpává kapacitu správce sítě opakovanými rutinními činnostmi a nedává časový prostor pro systematický a koncepční rozvoj a podporu uživatelů.
Škola v současné době provozuje převážně síťové přepínače Zyxel a HP. Vzhledem k cílům a požadavkům škola požaduje výměnu všech potřebných prvků pro zajištění centralizované správy a její sjednocení do jednoho administračního rozhraní.

Aktuální Wi-Fi systém nemá centralizovanou správu, má nedostatečný výkon a také slabé pokrytí. Škola požaduje moderní a bezpečné řešení, s ohledem na dnešní nároky. Současné prvky mimo jiné nepodporují aktuální bezpečnostní standardy (WPA3 apod.) ani pokročilé funkce optimalizace rádiového provozu a obsluhy připojených klientů. Není využíváno řízení přístupu klientů založené na standardu IEEE 802.1X.

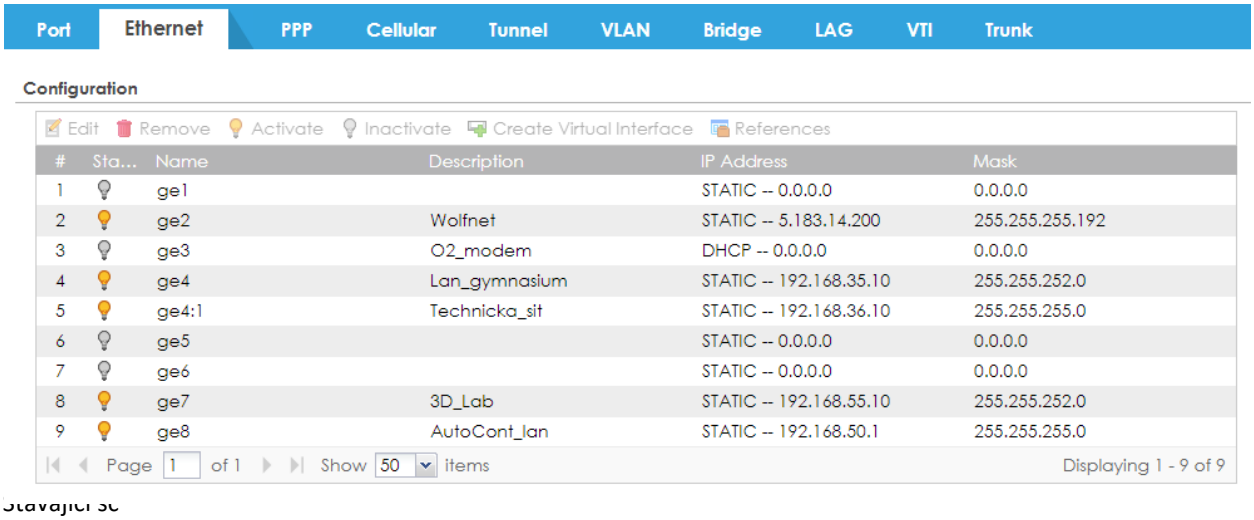
Zabezpečení přístupu k internetu a řízení provozu je realizováno standardním Zyxel firewallem, bez licencí a bezpečnostních funkcí jako například omezení přístupu na webové stránky.
Škola provozuje dosluhující server, bez podpory, na virtualizaci Hyper-V. Provozuje zde Active Directory, server Bakaláři a další. Zálohování škola řeší pomocí zastaralého diskového úložiště NAS.
V současné době škola spravuje identity jak v on-premisovém Active Directory, tak v cloudovém M365 prostředí. Aktuální záložní zdroje UPS jsou dosluhující.

Síť školy je v současné době realizována jako síť, která se postupným vývojem vyvinula z původně novellovské sítě do dnešní podoby sítě založené výhradně na MS technologiích a protokolu TCP/IP.
Síť je aktuálně obecně funkční, ale rychle zastarává, parametry nevyhovují výše zmíněnému Standardu konektivity škol a její budoucí rozvoj je bez výrazného zásahu do její struktury nerealizovatelný.
Síť pokrývá celý objekt gymnázia, přesněji pokrývá oba základní objekty gymnázia – pavilon A a pavilon B, částečně pokrývá objekt 3D laboratoře a učebny a vůbec nepokrývá venkovní prostory (hlavně hřiště a shromažďovací plochy). Částečně je pokryta tělocvična. Objekt jídelny též není pokryt a ani vůbec připojen.

Firewall a propojení sítě

Základem sítě je firewall, který řeší zabezpečené připojení školy k internetu a současně řeší routing mezi jednotlivými segmenty školní sítě.

Firewall je reálně reprezentován UTP firewallem ZyXEL ATP500, což je standardní firewall s pokročilými funkcemi, aktuálně s firmware V5.37 ABFU.0 Specifikace s detaily jsou k nalezení zde: https://shop.zyxel.cz/produkt/brana-zyxel-atp500
Jeho hlavním současným omezením je nevhodné programové vybavení pro budoucí zjevně násobně vyšší datové toky. Firewall není v HA clusteru, nemá aktivní placenou softwareovou podporu a jeho výpadek by kompletně paralyzoval síť školy (SPOF). Seznam aktivních sítí vypadá následovně:

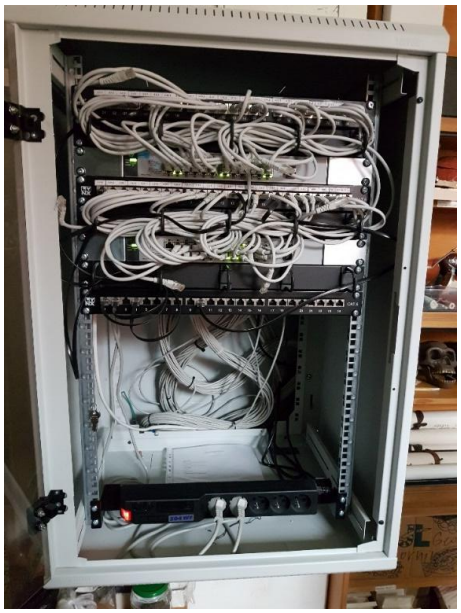


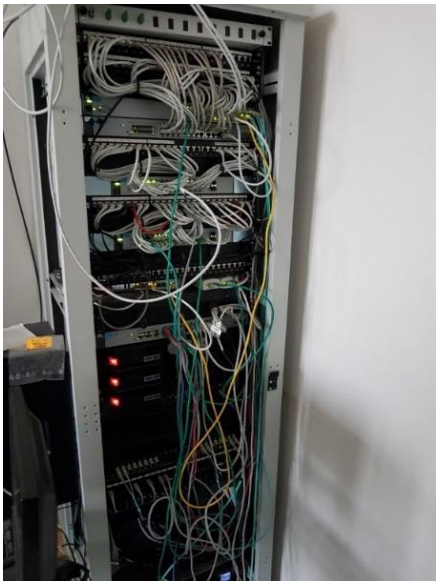
Stávající se

Schéma sítě v přehledu – pohled logického propojení včetně vyznačení pavilonů:

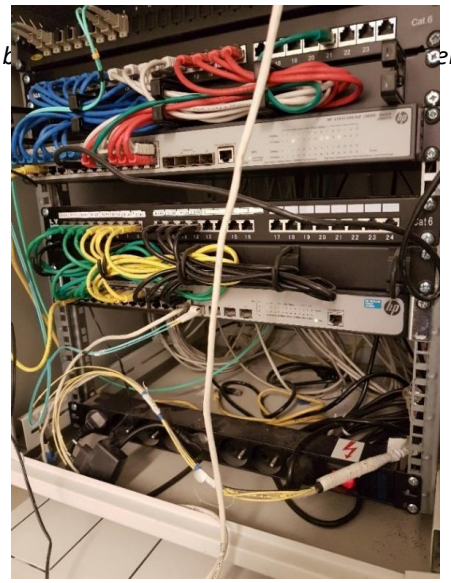
Vlastní propojení sítě je realizováno staršími switchi HP, které ale již jsou mimo období podpory, a hlavně jsou nejvýše gigabitové. Síť byla doplněna před dvěma lety dvojicí switchů ZyXEL XGS1530-52 která propojují pavilony A a B na 10Gb ale bohužel pouze po vadném optickém kabelu (byl poškozen při stavebních úpravách vstupní části školy a není přístupný), kde je funkční aktuálně pouze jedno vlákno a stav je havarijní . Současně platí, že z pohledu obsazenosti portů je síť zcela vytížená a v řadě pracovišť bylo postupně nutno doplnit místní malé switche, což sice řeší situaci, ale současně to znemožňuje a vylučuje další rozvoj, a hlavně realizaci VLAN.
Čistě technicky je třeba dodat, že stávající síť v pavilonu A je řešena jako síť s patrovými rozvaděči (dva na patro, jeden v druhém patře, osazeno starými switchi HP na 1 Gbitu) a v přípravně (VT1 DDT) je rack s technologií propojení a přívodem internetu.
Pavilon B je realizován jako kabelově jednotný s kabeláží svedenou do racku v přízemí v místnosti za bývalým bufetem, kde je umístěn stávající systém switchů a hlavní server v raccích
Propoj do 3D učebny je realizován optickým patch kabelem a spoj do tělocvičny taktéž.

Rack v





Rack v b ernetové lin



Pavilon A – patrové racky: (pro ukázku)

WiFi síť školy

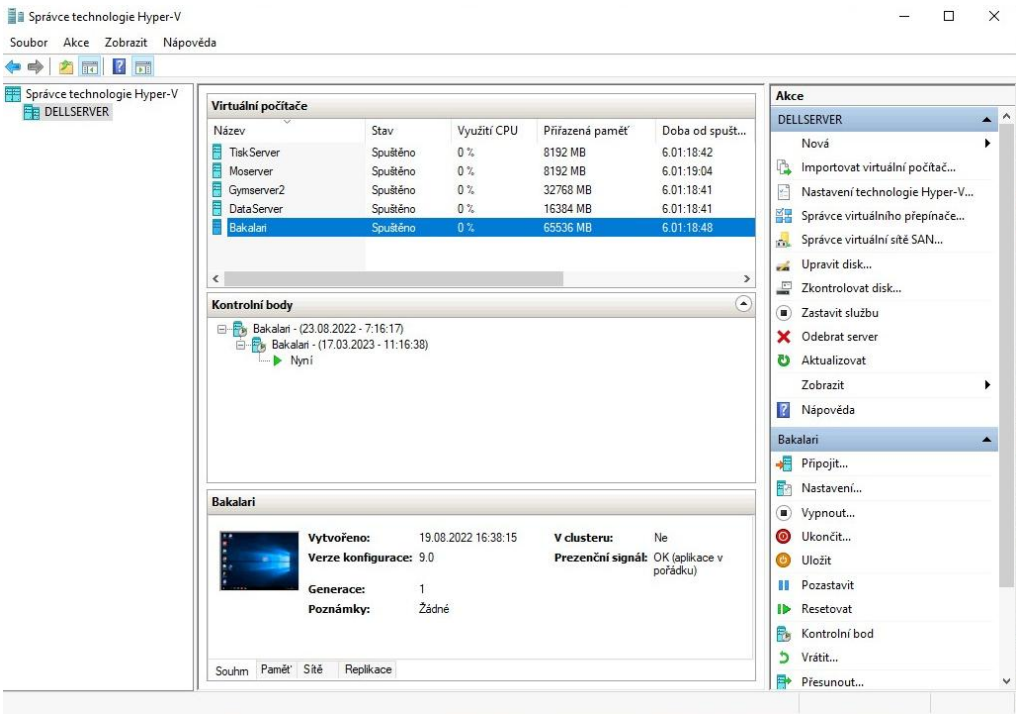
WiFi síť je realizována jako decentralizovaná pomocí jednotlivých WiFiAP , v pavilonu A je částečně již nahrazena několika AP Ubiquiti UniFi, ale o centrálně řízenou jednotnou síť tedy nejde.

Síť byla pořizována postupně, rostla pouze dle nutných požadavků s důrazem na nízkou cenu. Ukazuje se, že idea WiFi sítě pokrývající budouvu je velmi potřebná a byla by velmi využívaná, ale vzhledem k rychle rostoucí datové spotřebě nových zařízení je stávající síť aktuálně extrémně pomalá. Síť totiž pracuje výhradně v pásmu 2,4GHz a díky tomu je v současné době provozně přetížená až enormně přetížená. Současně také nepokrývá externí prostory školy hlavně tedy hřiště a odpočinkovou/shromažďovací plochu „za školou“ ani tělocvičnu s jídelnou.

Serverová část sítě

Stávající síť je již realizována jako několik virtuálních serverů na Hyper-V technologii, ale na poměrně starých serverech, kam byly tyto servery přesunuty z původních fyzických PC serverů gymnázia.

Technicky jde o dva servery HP Proliant Ml30 G9 (šest let starý), HPE ML10 G9 (šest let starý), kde běží AD řadič domény gymnázia a jeho záloha a repasovaný Dell v rackovém provedení (jde o 2xXeon Gold 6134 na 3,2GHz, 384GB Ram, 12TB na Dell poli s SATA disky a OS Windows Standard 2019, kde běží pět virtuálních serverů na Hyper-V technologii, tedy všechny podstatné servery gymnázia, konkrétně:



Je zřejmé, že výpadek serveru Dell, coby jediného nosiče kritických technologií gymnázia by způsobil kompletní výpadek sítě gymnázia, jde tedy o jasný SPOF.

Zálohy serverů se v současné době řeší pomocí free verze (community edition) sw. Veeam V12 na úložiště Synology DS420+ s 2x4TG HDD po 1Gbit ethernetu, ale zálohují pouze klíčové servery, nic jiného.

Provozně v současné době servery vyhoví, ale další zvýšení provozu již není možné. Současně není možné realizovat projekt virtualizace stanic (není to možné ani výkonově, ani kapacitou úložiště).
Současně je limitní doba záloh, hlavně pro značnou velikost uložených obrazů stanic pro výuku.

Shrnutí a rekapitulace plnění standardu konektivity

Přehled plnění standardu konektivity k 30.9.2024

Parametr	Požadavek na 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, v rámci projektu bude zachováno stávající připojení.
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.**
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.**
Schopnost snadné/automatické rekonfigurace pravidel firewallu (access listů) na základě identifikovaných útoků.	Ano	Tento parametr škola v současné době **nesplňuje.**
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.**
Validující DNSSEC resolver na straně školy, nebo poskytovatele konektivity, nebo otevřeným DNSSEC validujícím resolverem	Ano	Tento parametr škola v současné době **nesplňuje.**
Software a firmware je aktualizován po dobu udržitelnosti projektu, jsou-li aktualizace k dispozici	Ano	Tento parametr škola v současné době **nesplňuje.**
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.**
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.**
Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém	Ano	Tento parametr škola v současné době **nesplňuje.**
Systémy zálohování a obnovy dat serverové infrastruktury	Ano	Tento parametr škola v současné době **nesplňuje.**
Systémy pro antivirovou ochranu počítačových systémů, antispamovou ochranu poštovních serverů	Ano	Tento parametr škola v současné době **nesplňuje.**

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.**

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.**
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.**
Strukturovaná kabeláž pro připojení počítačových systémů a dalších zařízení (tiskárny, servery, AP aj.).	Ano	Tento parametr škola v současné době **nesplňuje.**
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.**
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.**
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.**

Zajištění vzájemně oddělených sítí pro zaměstnance školy, žáky/studenty školy a externí zařízení (hosty).	Ano	Tento parametr škola v současné době **nesplňuje.**
Podpora mechanismu izolace uživatelů.	Ano	Tento parametr škola v současné době **nesplňuje.**
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.**
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.**
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.**

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.**
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.**
Doporučená podpora pro ověřování uživatelů oproti databázi účtů [např. pomocí protokolu	Ano	Tento parametr škola v současné době **nesplňuje.**
IEEE 802.1X vůči centrální evidenci uživatelů (např. LDAP, MS AD) nebo pomocí Captive portalu].		Tento parametr škola v současné době **nesplňuje.**
Propojení aktivních prvků a důležitých systémů (např. Servery, NAS, propojení budov) rychlostí 10 Gbps, včetně uplinku.	Ano	Tento parametr škola v současné době **nesplňuje.**
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.**
Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management).	Ano	Tento parametr škola v současné době **nesplňuje.**
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.**
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.**

Zavedení více-faktorové autentizace.	Ano	Tento parametr škola v současné době **nesplňuje.**

Popis cílového stavu a specifikace předmětu plnění

Obecná specifikace

Vzhledem k předchozím specifikacím stávajícího stavu a podmínce, aby síť školy splňovala jako minimum „Standard konektivity škol“ a „Bezpečná digitální infrastruktura školy“ a současně, aby síť byla plně připravena na budoucí nároky a změny, požaduje zadavatel dodat koncepční a komplexní řešení řešení.

Zadavatel požaduje zjednodušení správy všech prvků – sjednocení správcovských konzolí a umožnění vytvoření moderní a bezpečné sítě a jednoduché obsluhy. Dále je požadován spolehlivý log management, bezpečný zálohovací nástroj, ověřování přístupu do sítě pomocí 802.1x, sjednocení současného on-premise Active Directory a M365 Active Directory, výměnu stávajících dosluhujících UPS a kompletní revize LAN sítě.

Zadavatel požaduje řešení, které nabízí centrální správcovskou konzoli jak pro next-gen firewall, tak pro síťové přepínače a přístupové WiFi body. Tato konzole musí být z bezpečnostních důvodů přístupná pouze prostřednictvím připojení VPN, které bude ošetřené dvou faktorovým ověřením (například přes mobilní aplikaci via OTP). Konzole musí umožňovat granulární kontrolu přístupových oprávnění (RBAC) – „admin“ bude smět provádět všechny operace v rámci konfigurace sítě/bezpečnosti, ale uživatel „dohled“ bude mít přístup pouze k přehledu správy přístupových bodů, nebo přepínačů. Zatímco například uživatel „reditel“ bude mít přístupný pouze přehled navštěvovaných webových stránek a bezpečnostních událostí.

V rámci řešení projektu zadavatel požaduje dodání dedikovaného nástroje pro log management. Tento nástroj bude provádět sběr logů/událostí ze všech dodaných síťových prvků (přístupové body, přepínače, firewall), hypervizoru, NAS, Active Directory, serveru. U nástroje pro log management požadujeme dedikovaný HW a úložiště. Nástroj musí být vybaven předdefinovanými dashboardy pro jednoduchou orientaci v událostech, musí provádět automatizovaný parsing událostí, automatizovanou korelaci dat (například pro upozornění pro mnoho neúspěšných loginů do sítě následovaných loginem úspěšným), schopnost zálohovat na externí úložiště, RBAC pro definici rolí, jednotný management, podporu od výrobce, alespoň jeden rok softwarové podpory a pět let podpory na dodaný HW. Zároveň Zadavatel požaduje podporu zálohování mimo nástroj samotný, pro navýšení času sběru událostí.

Zadavatel dále požaduje nakonfigurovat síť LAN v objektech zadavatele prostřednictvím nových aktivních prvků a nastavit v LAN tři VLAN pro učitele, žáky a management zadavatele s tím, že každá VLAN bude mít vlastní bezpečnostní politiku na firewallu.

Podstatnou částí dodávky je kompletní migrace stávajících virtuálních serveru ze stávajícího HW na nový server, dále zajištění Synchronizace lokálního MS Active Directory s Microsoft 365, zajištění logovacího nástroje a další implementační služby.

Základní požadavky technického řešení

Zadavatel požaduje, aby po realizaci projektu a po dobu udržitelnosti projektu (5 let) byl naplněn Standard konektivity školy a rozšířena funkčnosti ICT prostředí školy.

Dílčí cíle jednotlivých komodit jsou specifikovány následovně:

Specifikace komodit

Označení	Komodita
K1	Firewall
K2	Síťové přepínače
K3	Přístupové body
K4	Server
K5	Zálohování
K6	Logování
K7	UPS
K8	Bezpečnost
K9	Software
K10	Kabeláž
K11	Doprovodná část projektu
K12	Školení obsluhy a dokumentace

Zadavatel požaduje zachovat stávající softwarové serverové i desktopové platformy Microsoft pro zachování kompatibility se stávajícími systémy a výukovými a provozními aplikacemi.

Pokud dodavatel v rámci plnění projektu 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.

Pokud nabízené řešení dodavatele 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.

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

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

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.

Specifické požadavky na technické řešení

K1 – FIREWALL

Zadavatel požaduje dodávku **2 ks** Firewallu

zapojených v HA clusteru (typ clusteru není klíčový, active/active i active/pasiv je vyhovující) – dále jen FW.

Zadavatel požaduje aby FW splnil následující požadavky a parametry:

- Na FW budou ukončené všechny L3 Gatewaye a bude podporovat pokročilé bezpečnostní funkce.
- FW bude zároveň sloužit jako kontrolér pro síťové přepínače, tak pro přístupové body bezdrátové sítě
- FW bude připojen do agregačního switche pomocí SFP/SFP+ SR transceiverů a Multimode optického vlákna typu OM4.
- Připojení FW bude řešeno Port Channelem s protokolem LACP a tyto porty budou nastaveny v režimu non-negotiated trunk.
- FW musí podporovat Systém ochrany IPS – signatury striktně síťových útoků a vzory doprovodných anomálií, navíc konfigurovatelné pomocí zásad a senzorů.
- FW musí podporovat Filtr obsahu v síti, který chrání před škodlivými webovými stránkami a umožňuje blokovat webové stránky kvůli nežádoucímu obsahu (např. hazardní hry, pornografie, internetové obchody atd.)
- FW musí podporovat Podpora VPN – umožňuje vytvářet bezpečné a snadno použitelné VPN tunely (IPsec a SSL) na základě integrace s AD nebo jinými řešeními SSO. Alespoň pro 2 uživatele/adminy požadujeme dvou faktorové ověření pomocí OTP (HW token nebo Aplikace do iOS/Android)
- FW musí podporovat Antivirová ochrana proti narušení UTM – nejen pevné signatury, ale také pokročilou heuristiku, monitoring P2P a detekce virů z webových stránek.
- FW musí podporovat funkce sandboxingu pro detonaci podezřelých souborů v bezpečném odděleném cloudovém prostředí.

Součástí dodávky Firewallu bude:

- Instalace firewallu do racku
- Základní SW instalace firewallu do LAN/WAN zadavatele
- Konfigurace VLAN a LAN
- Nastavení základních bezpečnostních pravidel dle požadavku školy
- Migrace bezpečnostních pravidel ze stávajícího FW zadavatele
- návrh vylepšení na základě best practices a možností, které firewall nabízí
- Základní dokumentace nastavení firewallu
- Školení obsluhy na management firewallu
- Hardwarová a softwarová podpora výrobce min. 5 let, formou přednostního odbavení reklamačního procesu v případě poruchy.

Minimální technická specifikace firewallu

Požadovaná softwarová podpora	5 let
Požadovaná hardwarová podpora	5 let
Odeslání náhradního zařízení max. následující den po nahlášení závady	Ano
Počet portů síťových	10
Počet portů pro správu (konzole)	1
Počet portů SFP	2
Počet USB 3.0 portů	1
Podpora redundantního napájení	Ano
TPM modul	Ano
Propustnost IPS	1,3 Gbps
Propustnost se zapnutou ochranou	800 Mbps
IPv4 čistá firewall propustnost	9,5 Gbps
Min. počet session	1,4 milionu
Podpora SSL inspekce	Ano
Podpora IPsec/SSL VPN	Ano i Ano
Podpora více faktorového ověření administrátorů	Ano, součástí dodávky budou potřebné licence k aktivování OTP pro min. 2 admin účty
Podpora centrální správy prvků, jako přepínač a přístupový bod	Ano
Min. počet spravovaných přístupových bodů	94
Min. počet spravovaných přepínačů	22
Podpora Anti-spamu	Ano
Podpora kategorizace a blokování přístupu na škodlivé webové stránky	Ano
DNS inspekce	Ano
Plná podpora IPv4 i IPv6	Ano i Ano
Možnost napojení na cloudový sandbox	Ano
SNMP monitoring	Ano, verze v3
Syslog output	Ano
Detekce sítí botnet	Ano
Detekce podezřelých stránek	Ano
Podpora režimu HA	Ano, A/P i A/A

K2 – SÍŤOVÉ PŘEPÍNAČE

Zadavatel požaduje:

- prostřednictvím přepínačů (dále jen switch) realizovat kompletní propojení LAN školy tak, aby každý síťový prvek byl centrálně dohledatelný (z jednoho nástroje) a aby centrální konektivita jak mezi switchi tak i mezi switchi a serverem byla již na 2x10 Gbit pomocí optiky.
- switche budou mít propojení mezi sebou minimálně agregovanou linkou 2x10Gbit/s, nejhůře 1x 10Gbit (v případě výpadku jednoho SFP+ modulu).
- část switchů (viz specifikace níže) musí podporovat POE, pro pokrytí power budgetu požadovaných přístupových bodů.
- switche budou instalovány do racků ve stávajících technických místnostech
- switche budou propojeny navzájem optickými kabely pomocí :
    - -SFP+ transceiver 10GBASE-SR/SW - multirate, MM, OM3-300/OM2-82/OM1-33m, 850nm VCSEL, LC duplex, DMI (předpokládáme 32 ks)
    - SFP+ transceiver 10GBASE-T 10Gbps, 10GBASE-T, do 30m (CAT 6A či 7), RJ-45 (předpokládáme 8ks pro uplinky mezi jednotlivými switchi)

Součástí dodávky Switchů bude:

- Instalace switchů ro racků v technických místnostech
- Základní SW instalace switchů do LAN

- Nastavení páteřních switchů a základních VLAN dle požadavku školy
- Přepojení všech stávajících koncových bodů v LAN (PC v učebnách, kabinetech tiskárny atd.) do nových switchů
- Nastavení switchů pro stávající systémy zadavatele (kamery, telefony docházka, atd.)
- Základní dokumentace k jednotlivým prvkům a nastavení LAN
- Školení obsluhy na management switchů
- Hardwarová a softwarová podpora výrobce min. 5 let, formou přednostního odbavení reklamačního procesu v případě poruchy.

Zadavatel požaduje dodat následující typy switchů:

1 ks switch A - Agregační switch - 48 SFP+

Switch bude splňovat následujíc parametry:

- Layer 2/3 minimálně .48 x GE/10GE SFP/SFP+ slotů + min. 6 x 40GE QSFP+ nebo 4 x 100GE QSFP28
- možnost připojení i metalické kabeláže pomocí speciálních transceiverů.
- umožní připojit všechny ostatní dodávané switche a server/storage
- v L2 Spanning Tree topologii bude mít tento switch úlohu Root Bridge.
- ochranu před nežádoucí změnou STP topologie prostřednictvím Root Guard a BPDU Guard.
- verze Spanning Tree bude per-VLAN RSTP.

Minimální technická specifikace switche

Požadovaná softwarová podpora	5 let
Požadovaná hardwarová podpora	5 let
Centralizovaná správa	Ano
Health Monitoring	Ano
IGMP Snooping	Ano
Policy-Based Routing	Ano
Software update z konzole	Ano
Spanning Tree Protocol	Ano
802.1X	Ano
Monitoring klientů	Ano
DHCP Snooping	Ano
DHCP/ARP Monitor	Ano
Detekce klientů	Ano
Podpora automatizace, například pro blokaci klienta	Ano
Podpora protokolu LAG	Ano
Loop Guard	Ano
Podpora VLAN	Ano
ECMP	Ano
Podpora VXLAN	Ano
ACL	Ano, min. 4K
Dynamické routovací protokoly:	OSPF, RIP, VRRP, BGP, ISIS
Podpora netflow	Ano

3 ks switch B – přístupový 48 portový switch s podporou PoE+

Switch bude splňovat následujíc parametry:

- Layer 2 PoE+ min. 48x 1G RJ45 + min. 4x 10G/1G SFP+/SFP. Min. 24 portů s podporou PoE+
- Minimální celkový power budget pro POE 370W

- Metalické downlink porty s rychlostí 1Gbit
- jako uplinky do agregačního switche budou využity dedikované uplink porty SFP+
- každý switch bude připojen redundantně – MM optikou agregovaně 2x10Gbit
- plný management pomocí GUI i CLI rozhraní
- Podporu standardu 802.1Q pro segmentaci LAN sítě
- CAM table min.kapacita 32 tis. záznamů v MAC Address tabulce
- Switch bude podporovat Access listy pro přístup do administrace

Minimální technická specifikace switche

Health Monitoring	Ano
IGMP Snooping	Ano
Link Aggregation Configuration	Ano
LLDP/MED	Ano
Spanning Tree	Ano
Podpora LAG	Ano
802.1X Podpora	Ano
Detekce klientů	Ano
DHCP Snooping	Ano
DHCP/ARP Monitor	Ano
Automatizace, například pro blokaci klientů	Ano
Podpora ACL	Ano
Podpora netflow	Ano

4 ks switch C - přístupový 24 portový switch bez PoE

Switch bude splňovat následujíc parametry:

- Layer 2 switch min. 24x 1G RJ45 + min. 4x 10G/1G SFP+/SFP portů
- Metalické downlink porty s rychlostí 1Gbit
- Jako uplinky do agregačního switche budou využity dedikované uplink porty SFP+
- Každý switch bude připojen redundantně – MM optikou agregovaně 2x10Gbit
- Použitá optická vlákna budou typu OM4 (max délka 550m pro 10Gbit)
- Požadujeme plnou spravovatelnost pomocí GUI i CLI rozhraní
- Podporu standardu 802.1Q pro segmentaci LAN sítě
- CAM table min.kapacita 32 tis. záznamů v MAC Address tabulce
- Switch bude podporovat Access listy pro přístup do administrace

Minimální technická specifikace switche

Health Monitoring	Ano
IGMP Snooping	Ano
Link Aggregation Configuration	Ano
LLDP/MED	Ano
Spanning Tree	Ano
Podpora LAG	Ano
802.1X Podpora	Ano
Detekce klientů	Ano
DHCP Snooping	Ano
DHCP/ARP Monitor	Ano
Automatizace, například pro blokaci klientů	Ano
Podpora ACL	Ano
Podpora netflow	Ano

4x switch D – přístupový 24 portový switch s podporou PoE+

Switch bude splňovat následujíc parametry:

- Layer 2 PoE+ min. 24x 1G RJ45 + min. 4x 10G/1G SFP+/SFP portů. Min. 12 portů s podporou PoE+
- Minimální celkový power budget pro POE 185W
- Metalické downlink porty s rychlostí 1Gbit
- Jako uplinky do agregačního switche budou využity dedikované uplink porty SFP+
- Každý switch bude připojen redundantně – MM optikou agregovaně 2x10Gbit
- Použitá optická vlákna budou typu OM4 (max délka 550m pro 10Gbit)
- Požadujeme plnou spravovatelnost pomocí GUI i CLI rozhraní
- Podporu standardu 802.1Q pro segmentaci LAN sítě
- CAM table min.kapacita 32 tis. záznamů v MAC Address tabulce
- Switch bude podporovat Access listy pro přístup do administrace

Minimální technická specifikace switche

Health Monitoring	Ano
IGMP Snooping	Ano
Link Aggregation Configuration	Ano
LLDP/MED	Ano
Spanning Tree	Ano
Podpora LAG	Ano
802.1X Podpora	Ano
Detekce klientů	Ano
DHCP Snooping	Ano
DHCP/ARP Monitor	Ano
Automatizace, například pro blokaci klientů	Ano
Podpora ACL	Ano
Podpora netflow	Ano

3 ks switch E - přístupový 48 portový switch bez PoE

Switch bude splňovat následujíc parametry:

- Layer 2 min. 48x 1G RJ45 + min. 4x 10G/1G SFP+/SFPportů
- Metalické downlink porty s rychlostí 1Gbit
- Jako uplinky do agregačního switche budou využity dedikované uplink porty SFP+
- Každý switch bude připojen redundantně – MM optikou agregovaně 2x10Gbit
- Použitá optická vlákna budou typu OM4 (max délka 550m pro 10Gbit)
- Požadujeme plný management pomocí GUI i CLI rozhraní
- Podporu standardu 802.1Q pro segmentaci LAN sítě
- CAM table min.kapacita 32 tis. záznamů v MAC Address tabulce
- Switch bude podporovat Access listy pro přístup do administrace

Minimální technická specifikace switche

Health Monitoring	Ano
IGMP Snooping	Ano
Link Aggregation Configuration	Ano
LLDP/MED	Ano
Spanning Tree	Ano
Podpora LAG	Ano
802.1X Podpora	Ano
Detekce klientů	Ano
DHCP Snooping	Ano
DHCP/ARP Monitor	Ano
Automatizace, například pro blokaci klientů	Ano
Podpora ACL	Ano
Podpora netflow	Ano

K3 – PŘÍSTUPOVÉ BODY (WIFI)

Zadavatel požaduje vytvoření školní bezdrátové WIFI sítě školy prostřednictvím přístupových bodů, dále jen AP.

Zadavatel požaduje instalaci celkem 70 ks AP

dle návrhu dodavatele, který vzejde z odborného posouzení v rámci první implementační části projektu.

Zadavatel předpokládá instalaci AP takto:

- Pavilon A: 32 ks AP
- Pavilon B: 31 ks AP
- 3D učebna/koridor : 5 ks AP
- Tělocvična: 2ks

Finální instalace AP bude provedena na základě analýzy současného stavu a prováděcí dokumentace v rámci I.etapy (viz smlouva a výzva č.5 – doba plnění zakázky)

Součástí dodávky AP bude:

- Instalace a montáž AP v rámci budov zadavatele
- Základní instalace AP do LAN,
- Nastavení základních SSID dle požadavku školy
- Oživení a základní konfigurace bezdrátové sítě školy
- Nastavení AP pro stávající systémy zadavatele (kamery, telefony docházka, atd.)
- Základní dokumentace k jednotlivým prvkům a nastavení LAN
- Školení obsluhy na správu AP a WIFI sítí
- Hardwarová a softwarová podpora výrobce min. 5 let, formou přednostního odbavení reklamačního procesu v případě poruchy.

Minimální technická specifikace AP

Požadovaná softwarová podpora	5 let
Požadovaná hardwarová podpora	5 let
Podpora WiFi 6E	Ano
Min. počet interních rádií	3
Min. počet interních antén	4
Podpora OFDMA	Ano

Integrovaný bluethooth	Ano
Síťové rozhraní pro připojení	2,5 Gbit
MDI/MDIX	Ano/Ano
Podpora POE	802.3at
MU-MIMO	Min. 2x2 MU-MIMO
Min. propustnost 1. rádia	570 Mbps
Min. propustnost 2. rádia	1200 Mbps
Min. propustnost 3. rádia	2400 Mbps
UL MU-MIMO	Ano
DL- MU-MIMO	Ano
Automatické skenování wifi pásma	Ano
Režim packet snifferu	Ano
Analyzátor spektra	Ano
Dedikované TPM	Ano

K4 – SERVER

Zadavatel požaduje dodávku 1ks serveru

s implementaci Windows Serverů na virtualizační platformě Hyper-V.

Prostředí serveru bude optimalizováno podle požadavků tak, aby bylo zajištěno následující:

- Provoz virtuálních serverů
- Provoz doménových služeb
- Provoz aplikace Bakaláři (cca 700 uživatelů)
- Lokální úložiště dat pro učitele (70 uživatelů)
- Lokální úložiště dat pro studenty (600 uživatelů)
- Lokální úložiště dat pro provozní a ekonomický úsek (20 uživatelů)
- Provoz Tiskové a souborové služby

Součástí dodávky bude:

- Instalace a montáž Serveru v rámci budov zadavatele
- Základní instalace serveru do LAN
- Základní instalace serveru a virtuálního prostředí
- Migrace stávajících virtuálních serverů a aplikací na nově dodanou serverovou platformu
- Základní dokumentace
- Školení obsluhy na management serveru
- Hardwarová a softwarová podpora výrobce min. 3 roky formou přednostního odbavení reklamačního procesu v případě poruchy.

minimální technická specifikace serveru

Požadovaná hardwarová podpora formou dalšího pracovního dne (NBD)	3 roky
Rozměr	2U do 19“ racku
Virtualizační platforma	Hyper-V
Procesor	Min 12 jader 2Ghz s možností doplnit druhý procesor
Paměť	Min. 256 GB RAM 5600MT/s,
Síťová konektivita	2x 1GbE, 2x 10Gbit SFP+ Lan
Min. počet slotů pro RAM	16
Min. počet slotů pro HDD	12
SSD pro OS	480
Podpora RAID	0/1/10/5/6/50/60
Min. diskový prostor	20 TB
Min. velikost cache pro RAID	8 GB

Redundantní zdroje	Ano
Redundatní ventilátory	Ano
Vzdálená správa	Ano – ILO/iDrac
Rack rail kit	Ano
Server bude dodán s požadovanými licencemi pro Windows Server v dostatečném množství	Ano

Zadavatel dále požaduje, aby v rámci dodávky serveru byla provedena:

Synchronizace lokálního MS Active Directory s Microsoft 365

Konkrétně zadavatel požaduje, aby

- prostředí Active Directory (dále jen AD) bylo propojeno se stávajícím prostředím Microsoft 365 (MS365) tak, aby správa uživatelských účtů v AD a MS365 byla prováděna pouze jednou a z jednoho uživatelského rozhraní.
- dodavatel zajistil připojení uživatelů do LAN prostřednictví koncových bodů (PC/tablet/mobil) k nové doméně tak, že se uživatel bude k PC přihlašovat stejným způsobem jako do Microsoft 365.
- dodavatel zajistil migraci uživatelských dat ze stávajících profilů AD a MS365
- dodaný proces Synchronizace lokálního MS Active Directory s Microsoft 365 byl funkční minimálně po dobu 5let
- dodavatel disponoval certifikáty na odbornost na integraci Microsoft 365 a Active Directory Domains Onpremise v tomto minimálním rozsahu:

    - Znalosti v oblasti Microsoft 365
        - 5 let zkušeností
        - Implementace obdobných řešení ve škole (minimálně 1x reference)
        - Znalosti pro učitele pro nastavení prostředí Microsoft 365
        - Certifikace Microsoft Certified Educator (MCE)

    - Znalosti Active Directory
        - 5 let zkušeností
        - Implementace podobných řešení ve firmách (minimálně 1x reference)
        - Certifikace Windows Server 2016 MCSA

    - Znalosti v oblasti HW, zálohování a virtualizace
        - 5 let zkušeností
        - Zkušenosti s elektroinstalací, konfigurací HW serveru, úložištěm.
        - Prostředí zálohování Veeam nebo ekvivalentní
        - Certifikace certifikovaného inženýra Veeam nebo ekvivalentní
        - Zkušenosti s instalací technologie Hyper-V

K5 – ZÁLOHOVÁNÍ

Zadavatel požaduje, aby prostředí virtuálních serverů bylo zálohováno pomocí moderního řešení a to včetně nastavení zálohovací strategie a retence. Nevyžaduje se zálohování Microsoft 365. Software pro zálohování bude virtualizován na nové serverové platformě, odtud bude napojen na diskové pole dodaného NAS, které bude využívat jako bezpečné oddělené úložiště záloh.

Součástí dodávky bude:

- Instalace a montáž HW pro zálohování dat (dále jen HWZ)
- Základní instalace HWZ do LAN

- Konfigurace zálohy virtuálních serverů
- Základní dokumentace HWZ
- Školení obsluhy na management HWZ
- Hardwarová a softwarová podpora výrobce min.5 let, formou přednostního odbavení reklamačního procesu v případě poruchy.

Minimální technická specifikace HWZ

Rozměr	NAS Rackmout
Min. počet jader CPU	4
Min. RAM paměť	8GB Ram
Síťová konektivita	1Gbit RJ45, 2x10Gbit SFP+
USB port pro propojení s UPS	Ano
Podpora iSCSI	Ano
Disková kapacita	48 TB
Rack rail kit	Ano
Vnitřní software pro Active Backup pro případ odlišných zálohovacích scénářů.	Ano
Podpora pro zálohování virtuálních strojů (VMs)	Ano
Podpora pro zálohování fyzických serverů a pracovních stanic	Ano
Podpora pro zálohování cloudových úložišť (AWS, Azure, Google Cloud)	Ano
Možnost granulární obnovy souborů a aplikací	Ano
Podpora pro zálohování NAS (Network Attached Storage)	Ano
Možnost replikace dat pro účely disaster recovery	Ano
Podpora pro zálohování Windows a Linux systémů	Ano
Možnost vytváření bootovatelných kopií záloh	Ano
Podpora pro zálohování a obnovu dat z Microsoft 365	Ano
Možnost zálohování až 10 pracovních úloh	Ano, 10

K6 – LOGOVÁNÍ

Zadavatel požaduje dodávku a implementace nástroje pro centralizované zaznamenávání událostí z libovolných zdrojů, s možností analýzy a řešení provozních i bezpečnostních událostí/incidentů ze systémů a aplikací zadavatele.

Požadujeme dodání uživatelsky přívětivého nástroje pro log management, který v budoucnu umožní jednoduché rozšiřování sběru událostí. Například jednoduchým přidáním IP adresy do nastavení systému, nebo instalací agenta na koncový počítač/server, bez nutnosti složité konfigurace, nejlépe formou jednoduchého instalačního průvodce.

Požadujeme navrhnout, dodat a implementovat nástroj na zaznamenávání událostí. Tento nástroj bude sloužit pro sběr a analýzu logů s možností následné analýzy a řešení bezpečnostních událostí/incidentů ze systémů a aplikací zadavatele určeným hodnocením aktiv a bezpečnostních potřeb školy. Navržený nástroj musí zachovávat originál logů za účelem bezpečnostního auditu. Nástroj musí být dále schopen zajistit přesné časové razítko ke všem pořízeným událostem a umožnit zachování důvěrnosti a integrity pořízených dat po celou dobu jejich životního cyklu. Pro efektivní využití musí nástroj umět generovat reporty o aktivitách systémů i uživatelů, včetně auditních reportů na vyžádání, nebo se stanovenou periodicitou s definovatelným obsahem – například řediteli o požadovaných provozních informací.

Požadujeme, aby nástroj měl jednotné úložiště logů s pokročilými nástroji analýzy a upozorňování, ke kterému budou mít přístup pouze autorizovaní pracovníci zadavatele. Nezbytnou nutností je vyloučit možnost modifikace logů ze strany administrátorů nebo uživatelů. Nástroj musí dále umožňovat snadnou klasifikaci dat, tvorbu uživatelsky definovaných parserů, filtrů, upozornění a korelací bez účasti výrobce nebo dodavatele ve snadno pochopitelném grafickém rozhraní bez nutnosti používat znalostí programátora. Dokumentace musí poskytnout jednoznačný návod, jak takovéto činnosti provádět, a to včetně široké škály vzorových příkladů. Zálohování

konfigurace i dat a jejich obnova je nezbytnou nutností, kterou musí dodaný systém podporovat zálohování dat na externí systém.

Požadujeme aby, nabízený nástroj splňoval očekávané parametry uživatelské přívětivosti a integrity uživatelského rozhraní a vyhnout se nutnosti používaní skriptů, maker, konfigurací v příkazové řádce nebo terminálu. V případě pochybností o vlastnostech nabízeného nástroje si vyhrazujeme právo vyžádat funkční vzorek nabízeného řešení pro ověření funkčních vlastností a provést ověřovací testy ještě před ukončením výběrového řízení. V tomto případě je dodavatel povinen dodat funkční vzorek s technickými parametry nabízeného řešení do 1 týdne od výzvy zadavatele a poskytnout součinnost s testováním. Dále si vyhrazujeme právo vyžádat kontakty alespoň na 3 referenční zákazníky z našeho sektoru pro účely zjištění zkušeností s nabízeným systémem.

Součástí dodávky bude:

- Instalace a montáž HW a SW pro logování (dále jen HSL)
- Základní instalace HSL do LAN školy
- Konfigurace HSL dle požadavků zadavatele
- Základní dokumentace HSL
- Školení obsluhy na management HSL
- Hardwarová a softwarová podpora výrobce HW min.5 let a SW 1rok formou přednostního odbavení reklamačního procesu v případě poruchy.

Minimální technická specifikace HSL

Požadovaná softwarová podpora	Min. 1 rok
Požadovaná hardwarová podpora	5 let
Systém bude řešen jako hardwarová appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů. Nutno doložit katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry nabízeného systému.	Ano
Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware.	Ano
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.	Ano
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. Nutno předložit příslušnou dokumentaci k vytváření parserů a testování jejich funkčnosti.	Ano
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.	Ano
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.	Ano
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.	Ano
Hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a standardizovat alespoň na tyto	Ano

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.	Ano
Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.	Ano
Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.	Ano
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.	Ano
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.	Ano
Systém provádí konsolidaci logů na interním storage logovacího systému.	Ano
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.	Ano
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.	Ano
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.	Ano
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.	Ano
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.	Ano
V případě krátkodobého (do 10 minut) až dvounásobného 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.	Ano
Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno,zdrojová IP, značka/tag apod.).	Ano
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.	Ano
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.	Ano
Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.	Ano
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.	Ano
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.	Ano
Systém umožňuje kapacitní i výkonovou škálovatelnost.	Ano
Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 4TB. V ražimu RAID 1.	Ano
Pokročilá telemetrie a monitoring stavu systému. Systém musí umět zobrazovat kromě běžných telemetrických dat o svojí činnosti i data ohledně rychlosti indexování, délce fronty dat čekající na zpracování a rychlosti odezvy DNS serverů vyřizujících DNS PTR odpovědi. Dále musí umožňovat alertování při překročení prahových hodnot nebo chybě systému, s odesláním upozornění pomocí SMTP nebo Syslogu.	Ano
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.	Ano
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.	Ano
Dodaný systém musí obsahovat ucelené all-in-one řešení pro parsování a normalizaci přijatých událostí bez nutnosti	Ano

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.	Ano

Minimální HW požadavky pro řešení HSL

Velikost	Desktop
HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) pro svoji činnost a je nezávislá na dalších systémech.	Ano
CPU	Min. 1 CPU, 16 jader, 2,8 Ghz
RAM	Min. 64 GB
Minimální velikosti integrované databáze	Min. 4 TB
Síťové rozhraní	Min. 1x Gbit RJ-45

Minimální výkonové a softwarové požadavky pro řešení HSL

Systém funguje formou HW appliance (všechny části systémů je možné nastavit v centrální webové konzoli a není nutné editovat žádné konfigurační soubory, scripty nebo makra v příkazové řádce).	Ano
Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správcovskou konzoli. Všechny aktualizace musí být prováděny z webového prostředí bez potřeby asistence dodavatele/výrobce dodávaného systému. Požadujeme předložení posledních 4 poznámek k novému vydání (release notes) pro kontrolu parametrů navrhovaného systému.	Ano
Systém musí podporovat downgrade v jednom kroku, pro případ problémů s novou verzí systému po upgrade. Není přípustný downgrade pouze za součinnosti výrobce. Popište podrobně způsob realizace downgrade, nebo přiložte odkaz na dokumentaci s detailním popisem.	Ano
Průměrný trvalý příjem min. 1000 událostí/s. Výkon musí být dosažen na požadované množství událostí s průměrnou délkou zpráv minimálně 700Byte trvale. Systém musí prokazatelně kompletně zpracovat přijaté události včetně vytváření očekávaných metadat (DNS-PTR, čísla a jména ASN, geolokace), zajišťovat normalizaci, zamezovat ztrátě přijatých událostí nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu každé události.	Ano
Špičkový příjem minimálně 2000 událostí/s po dobu nejméně 10 minut a průměrnou délkou minimálně 700byte. Systém musí prokazatelně kompletně zpracovat přijaté události, zamezovat ztrátě ukládaných dat nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu zpráv. Při zpracování dat během špičkového příjmu akceptujeme zpoždění zobrazení zpracovávaných dat. Systém ani ve špičkovém výkonu nesmí dovolit ztrátu dat, skluz důvěryhodného časového razítka nebo jiné prokazatelné vady na zpracovávaných datech oproti zpracování při průměrném trvalému příjmu událostí.	Ano
Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB. Integrovaná databáze musí mít čistou velikost nejméně 4 TB a nad to musí podporovat kompresi ukládaných dat.	Ano
Uživatelská konfigurace klasifikace dat, parserů, filtrů a alertů se provádí pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk musí uživateli umožnit psát konfigurace bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou schémat-symbolů, které reprezentují aplikační logiku a kontrolují syntaxi. Doložte odkazem na dokumentaci systém vizuálního programování a popisu jednotlivých použitých komponent vizuálního programování nástroje.	Ano
Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, čísel a jmen autonomních sítí, geolokační informace a identifikace výrobce zařízení podle MAC adresy.	Ano
Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů požadujeme mít možnost vložení minimálně 20 testovacích zpráv současně. Doložte odkazem na dokumentaci, ze které je zřejmé, jakým způsobem se vkládají testovací zprávy během psaní nového uživatelského parseru a jakým způsobem je prezentován výstup testu.	Ano
V centrální správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. Systém obsahuje předdefinované značky, které automaticky přidává k přijímaným zprávám. Příklady značek: konfigurační změna, úspešné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla z windows, zpráva byla vygenerována firewallem atd...	Ano
Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem.	Ano
Systém musí umožňovat export dat ve formátu vhodném pro další strojové zpracování bez dodatečných omezení na časové období, množství nebo obsah exportovaných dat. Během exportu je možné označit pouze vybraná pole, která mají být do exportu zahrnuta.	Ano
Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém. Doložte odkazem na dokumentaci, jakým způsobem se provádí zálohování a obnova konfigurace systému.	Ano
Podpora důvěryhodného zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány a umožnit v budoucnosti obnovení bez ohledu na verzi systému, ve které byla záloha pořízena. Doložte odkazem na dokumentaci, jakým způsobem se realizuje zálohování a obnova záloh.	Ano

K7 – UPS

Zadavatel požaduje dodat řešení pro zálohování napájení serveru a zálohovacího řešení (dále jen UPS)
V rámci projektu požadujeme dodání 2 kusů UPS, dostatečně dimenzovaných pro pokrytí napájení potřebných síťových prvků.

Součástí dodávky bude:

- Instalace a montáž UPS
- Konfigurace UPS dle požadavků zadavatele
- Základní dokumentace
- Školení obsluhy
- Hardwarová a softwarová podpora výrobce HW min.5 let formou přednostního odbavení reklamačního procesu v případě poruchy.

Minimální technická specifikace

Minimální kapacita	2200 VA
Provedení rackmount	Ano
Uživatelsky vyměnitelná baterie	Ano
Možnost propojení se serverem	Ano
Self Test	Ano
Zvukové výstrahy v případě poruchy	Ano
Přepěťová ochrana	Ano
AVR	Ano
Podpora aktivního PFC	Ano

K8 – BEZPEČNOST – 802.1x + ANTIVIROVÁ OCHRANA

Zadavatel požaduje, aby koncoví uživatelé a koncová zařízení byli v síti ověřování prostřednictvím protokolu 802.1x a dále požaduje implementaci antivirové ochrany pro 160 PC stanic a server.
Zadavatel požaduje

- Implementovat protokol 802.1x pro koncové stanice, které budou využívat technologie Microsoftu, prostřednictvím využití tunelované metody EAP-TLS s autentizací Machine certifikátem.
- Implementovat systém pro ověření klienta formou RADIUS server, který bude napojen na AD doménu. Jako RADIUS server bude využit technologii Microsoft NPS nebo FreeRADIUS
- Aby zařízení, která nejsou spravovaná školou byla ověřována pomocí metodu PEAP-MSCHAPv2
- Aby zařízení, která jsou spravovaná školou (Učitelé i žáci) byla ověřováni prostřednictvím RADIUS serveru v AD.
- implementaci antivirové ochrany pro 160 PC stanic a server - PC ve třídách, kabinetech a učebnách

Součástí dodávky bude:

- Instalace antivirového sw a implemenatce 802.1x do prostředí LAN
- Konfigurace sw dle požadavků zadavatele
- Základní dokumentace
- Školení obsluhy

Minimální technická specifikace

Ověřování do sítě pomocí 802.1X

Implementace všech potřebných částí a prací pro nasazení 802.1X	Ano

Antivirová ochrana

Ochrana v reálném čase proti malwaru	Ano
Automatické aktualizace definic virů	Ano
Správa hrozeb a zranitelností	Ano
Ochrana proti phishingu	Ano
Kontrola a skenování souborů a aplikací	Ano
Ochrana proti ransomware	Ano
Firewall a síťová ochrana	Ano
Ochrana cloudových úložišť	Ano
Ochrana proti exploitům	Ano

K9 – SOFTWARE

V rámci projektu požadujeme dodání 15 kusů MS Office LTSC Standard EDU (trvalá licence) v aktuální verzi.

K10 – KABELÁŽ

Zadavatel požaduje dodávku optických tras v rámci budov školy a dodávku nových metalických rozvodů v technických místnostech.

Zadavatel požaduje dodávku následujících optických tras:

A) Serverovna A - Serverovna B – celkem 160m – kvalita multimode 16 vlákno
B) Serverovna A - Serverovna VT2 – celkem 70m – kvalita multimode 8 vlákno
C) Serverovna A - Serverovna BIO – celkem 20m – kvalita multimode 8 vlákno
D) Serverovna B - Serverovna 3D – celkem 70m – kvalita multimode 8 vlákno

Celkem 320 m optického vedení. Vedení bude vedeno ve stávajících trasách (lištách) po povrchu s minimem průrazů. Optické trasy budou ukončeny v příslušných rack.

Zadavatel požaduje dodávku metalických tras pouze v režimu realizace úprav všech stávajících rack layoutů tak, aby byla strukturovaná kabeláž v každém racku přehledná a snadno trasovatelná.

Součástí dodávky bude:

- měření páteřních optických a metalických tras – předávací protokol
- závěrečná dokumentace aktuálního stavu síťového prostředí v elektronické podobě
- označení všech páteřních metalických a optických kabelů v rack

K11 – DOPROVODNÁ ČÁST PROJEKTU – dodávka HW

Zadavatel požaduje v rámci doprovodné části projektu dodávku HW pro upgrade HW v učebnách.

Konkrétně je požadována dodávka:

- 25 ks setu miniPC+LCD+Klávesnice+myš
- 25 ks LCD TV 86“
- 25ks vizualizer

Zadavatel v doprovodné části projektu nepožaduje montáž hardware.

Minimální technická specifikace

Mini PC – min. i3 CPU, 8 GB RAM, 256 GB SSD, 24“ IPS monitor, klávesnice, myš, Windows 11 Pro	Ano – 25 ks
TV - LCD 86" - SMART, LED, 218cm, 4K Ultra HD, 100 / 120 Hz, HDR10, DVB-T2/S2/C, 4× HDMI, 2× USB, USB nahrávání, LAN, WiFi, Bluetooth, DLNA, Miracast, HbbTV 2.0, hlasové ovládání, přehrávání 360° videa, Apple Airplay 2, párování s mobilním zařízením, WebOS, VESA 600×400, repro 20 W, AI Sound Pro, Dolby Digital	Ano – 25 ks
Vizualizer s flexibilním ramenem, výstup 3264 x 2448, USB, snímač min. 8 Mpx + kabeláž (HDMI 20m)	Ano – 25 ks

K - 11 ŠKOLENÍ A DOKUMENTACE NAD CELOU DODÁVKOU

Dodavatel provede pro každou komoditu 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 této veřejné zakázky, a to minimálně v rozsahu:

a) běžných administrátorských činností pro implementované systémy a HW
b) standardní údržby systémů pro administrátory zadavatele

Zadavatel zajistí školení v potřebném rozsahu pro zástupce zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.

Zadavatel požaduje, aby v rámci dodaného řešení byla předána i dokumentace ke každé dílčí
části K1 – K10 (kromě K9),

Dokumentace k celému projektu, která bude součástí dodávky musí být úplná a v češtině. Obsahem i kvalitou bude srovnatelná s aktuální dokumentací v angličtině. Není přípustné předložit českou dokumentaci, která bude odkazovat do dokumentace, která bude v jiném jazyce, než je čeština. Dále by dokumentace měla poskytnout jednoznačné návody, jak konfigurovat nejčastější zdrojová zařízení pro spolupráci s nabízeným systémem.

Záruky a servisní podmínky

Zadavatel požaduje následující záruky a servisní podmínky pro dodávky:

1. Zadavatel uvádí u jednotlivých komodit požadovanou min. záruku, záruční servis a podporu.
2. Pokud není uvedeno jinak je minimální záruka stanovena na veškeré dodávky 60 měsíců.
3. Z důvodu zajištění udržitelnosti projektu a zajištění bezpečnosti provozu po dobu 60 měsíců požaduje zadavatel poskytnutí prodloužených záruk pro některé komponenty, v jejichž popisu je informace o prodloužené záruce uvedena, při zachování ostatních parametrů původní záruky (rychlost opravy, rozsah aktualizací firmware apod.).

4. Zadavatel v rámci této technické specifikace požaduje specifické služby, které se odvíjejí od konkrétního typu plnění, a to zejména následující:
    a. záruka – záruku v intencích zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů, tedy, že si předmětné plnění po dobu záruky zachová své vlastnosti a parametry z doby jeho dodávky a dále, že po celou dobu záruky bude mít parametry a vlastnosti požadované objednatelem;
    b. prodloužená záruka – jedná se o záruku v intencích výše uvedené odrážky „záruka“ na dobu delší než standardní nebo obvyklou za dodržení parametrů a požadavků na záruku zařízení;
    c. záruční servis – záruční servis v parametrech konkrétního SLA (service level agreement) uvedeného u každého jednotlivého zařízení, u kterého je záruční servis požadován; předmětem záručního servisu je zajištění podpory provozu a odstraňování závad dodaných zařízení dodavatelem nebo výrobcem zařízení s garancí po požadovanou dobu;
    d. podpora – u části plnění spočívající v dodávce software a jejich licencí, kde není relevantní požadovat záruku ani záruční servis, požaduje objednatel technickou podporu daného software po dobu stanovenou vždy u konkrétního softwarového produktu; primární součástí takové podpory musí být nárok na opravné verze software a přístup k řešení problémů s takovým software, další specifické požadavky podpory jako nárok na veškeré nové verze nebo další požadavky jsou vždy konkrétně uvedeny u předmětné podpory a konkrétního software v této technické specifikaci.
5. Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro zadavatele.
6. Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.
7. 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.
8. Pro hlášení servisních požadavků zajistí dodavatel zadavateli přístup ke svému helpdeskovému systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení. Detailní popis helpdeskového systému a jeho obsluhy musí být součástí dokladů u předání díla. Provozní doba helpdeskového systému musí být minimálně 8–17 hod. v pracovních dnech.