Příloha č. 2 Zadávací dokumentace – Technická dokumentace zadavatele

Příloha č.1 Kupní smlouvy – Technická dokumentace kupujícího

# 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

Z důvodu kompatibility se stávající infrastrukturou a proškolených správců počítačové sítě, mohou být v zadávací dokumentaci uvedeny konkrétní značky výrobků, nebo určitý výrobce. Tyto důvody jsou vždy uvedeny v konkrétní části specifikace tam, kde dochází k uvedení konkrétního produktového názvu. V souladu s § 89 odst. 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, zadavatel připouští možnost dodávky rovnocenného řešení, které však musí zajistit celý komplex služeb, který je kompatibilitou vyžadován, tedy komplexní řešení agendových informačních systémů nad touto platformou vybudovaných a provozovaných, které předmětnou infrastrukturu užívají a slouží k výkonu veřejné správy zadavatele.

**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.

Plnění jednotlivých komponent dle specifikace níže je požadováno v následujícím rozsahu, a to včetně příslušenství:

|  |  |
| --- | --- |
| Položka plnění | Počet kusů |
| Firewall s příslušenstvím | 1 |
| Centrální přepínač včetně příslušenství | 1 |
| Přístupový přepínač 24 port včetně příslušenství | 2 |
| Přístupový přepínač 24 port PoE včetně příslušenství | 5 |
| Přístupový přepínač 48 port včetně příslušenství | 4 |
| Kontrolér | 1 |
| Vnitřní přístupový bod Wi-Fi 6 s příslušenstvím | 32 |
| Venkovní přístupový bod Wi-Fi 6 s příslušenstvím | 1 |
| Optické prvky | 1 sada |
| Nasazení federovaného systému Eduroam | 1 |
| Systém pro řízení přístupu založený na IEEE 802.1X | 1 |
| Systém pro sběr a správu logů a monitoring síťového provozu | 1 |
| Server s příslušenstvím | 1 |
| Záložní zdroj s příslušenstvím – pro server | 1 |
| Síťové úložiště s příslušenstvím pro ukládání záloh | 1 |
| Záložní zdroj s příslušenstvím – pro NAS | 1 |
| Záložní zdroj s příslušenstvím – pro přepínače | 3 |
| Licence zálohovacího software | 1 |
| Licence serverových operačních systémů | 1 |
| Přístupové serverové licence | 100 |
| Učitelský notebook | 25 |
| Dobíjecí vozík | 1 |
| Žákovský notebook | 25 |

# Popis současného stavu

Areál Základní školy Lomnice, okres Sokolov je umístěn na adrese Školní 234, Lomnice a skládá se z celkem pěti budov. V současné době navštěvuje školu 147 žáků a 26 zaměstnanců.

Obsah obrázku Letecké snímkování, strom, Urbánní design, mapa

Popis byl vytvořen automaticky

Realizace projektu bude probíhat ve všech využívaných objektech.

Současný stav ICT školy plně 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 až Cat5e bylo budováno a rozšiřováno postupně podle aktuálních potřeb a finančních prostředků školy. Bezdrátové připojení je realizováno na úrovni standardu Wi-Fi 4 a vyžaduje přestavbu. Aktivní prvky sítě jsou již technicky i morálně zastaralé a výrobci nepodporované (nebo jen omezeně). Chybí významná provázanost a centralizovaná správa infrastruktury sítě.

Kabelové rozvody byly provedeny kabely Cat5e. Pokrytí potřebných prostor budov metalickými rozvody je nedostatečné.

Aktuálně využívaný server výkonem a kapacitou vyhovuje aktuálním požadavkům, ale není schopen splnit všechny požadavky systému splňujícího požadavky Standardu konektivity.

Server je aktuálně připojen rychlostí 1Gb/s do páteřního switche.

Propojení stanic i serverů je zajištěno přepínači 1 Gb/s, z nichž některé jsou 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.

Internetové připojení je realizováno společností Rete internet s.r.o. bezdrátovým pojítkem s rychlostí 100 Mbps symetricky bez IPv6 konektivity. Rychlost připojení tak splňuje požadavek Standardu konektivity škol – 36,75 Mbps (147 žáků x 0,25 Mbps).

Škola má přidělenu veřejnou IP adresu IPv4 Škola nemá v současné době validující DNSSEC resolver na straně školy, neprovádí pokročilý monitoring provozu.

Škola provozuje Wi-Fi síť, které nepokrývá větší část školy a nesplňuje technologické požadavky kategorie Wi-Fi 5. Tato Wi-Fi síť není centrálně spravovaná a je potřeba ji modernizovat.

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

Zálohování serveru řídí prostředky operačního systému. Zálohy jsou ukládány na samostatný, lokálně umístěný disk odděleně od serveru. Kapacita je nedostatečná pro zálohování současného objemu dat a realizaci pokročilé ochrany záloh před kompromitací např. snapshoty či obdobnou technologií.

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

Přístup do počítačů (resp. operačních systémů) je řízen převážně ověřováním vůči doméně Active Directory.

Hlavní softwarovou platformou serverů i uživatelských počítačů jsou operační systémy společnosti Microsoft. Na koncových počítačích učitelů i žáků jsou používány převážně operační systémy Windows 10 a vyšší s podporou domény Active Directory. Škola provozuje aktuálně téměř 150 zařízení. Správa životního cyklu operačních systémů a aplikačního vybavení se provádí manuálně. Ochrana počítačů před škodlivým software momentálně není zajišťována, škola zajistí nákup vhodného SW prostředku před realizací tohoto projektu.

# Specifikace dodávaných technologií

V dále uvedených tabulkách jsou uvedeny povinné parametry prvků nabízeného řešení. Dodavatel musí všechny parametry splnit, v případě nesplnění požadavku zadavatele bude nabídka dodavatele vyřazena a dodavatel bude následně vyloučen z účasti v zadávacím řízení.

Dodavatel ve své nabídce detailně popíše způsob naplnění každého povinného parametru včetně značkové specifikace nabízených dodávek. Dodavatel tedy uvede konkrétní technické parametry nabízeného zboží, vč. uvedení výrobce a obchodního / typového označení jednotlivých komponentů. Údaje o výrobci a obchodním (či typovém) označení budou uvedeny a doloženy v tabulkách povinných parametrů; konkrétní parametry budou doloženy formou katalogových listů, nebo technických listů, v takovém případě ale musí být v tabulce odkázáno na část nabídky, ve které je možné naplnění parametru ověřit.

Popis způsobu naplnění každého povinného parametru bude konkrétní, úplný a musí výslovně prokazovat (nepostačuje pouze potvrzení či zkopírování požadavku Zadavatele), že nabízené řešení jednoznačně splňuje všechny aspekty povinného parametru. V případě nesplnění požadovaného způsobu prokázání plnění povinných parametrů bude účastník vyloučen z účasti v zadávacím řízení na danou VZ.

Vyplněné tabulky z tohoto oddílu technické specifikace učiní dodavatel součástí své nabídky, k nim pak přiloží případné další dokumenty obsahující technickou specifikaci nabízeného plnění (katalogové listy či technické listy) a prokázání plnění povinných parametrů.

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:

| **Komodita B – Zabezpečení LAN a Wi-Fi** | | | | |
| --- | --- | --- | --- | --- |
| **Část** | **Parametr** | **Popis povinného parametru** | **Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek** | **Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| **Firewall s příslušenstvím** | HW parametry | Počet síťových rozhraní LAN RJ45 1 Gbps – min 8x, 10 Gbps – min 2x, |  |  |
| Propustnost firewallu min. 20 Gb/s nezávisle na velikosti paketu |  |  |
| Výkon | Propustnost firewallu - min. 3 Mpps (pps - paketů za sekundu) |  |  |
| Počet FW politik min. 5 000 |  |  |
| Počet současných otevřených spojení – min 3 M |  |  |
| Propustnost VPN - min. 25 Gbps |  |  |
| Propustnost IPS – min 4,5 Gbps |  |  |
| Propustnost antiviru - min. 2 Gbps |  |  |
| Režim vysoké dostupnosti – Active Active, Active Passive, Clustering |  |  |
| Funkce | 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 routovacích protokolů – OSPF, PPTP, L2TP, GRE |  |  |
| Možnost nastavovat firewall politiku na základě geografických údajů. |  |  |
| Firewall | 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 |  |  |
| Možnost výběru mezi file based režimem (buffer) nebo flow based (inspekce on-the-fly) |  |  |
| Filtrační funkce | 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 |  |  |
| 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 200 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 |  |  |
| LDAP, Active Directory, Radius, TACACS+, Ověřování na základě certifikátu |  |  |
| Ověřování uživatelů | 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. |  |  |
| RIP, BGP, OSPF, IS-IS |  |  |
| Dynamické routování | 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 |  |  |
| Integrované logování a reporting, možnost vytváření vlastních reportů |  |  |
| 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. |  |  |
| **Centrální přepínač včetně příslušenství** | 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 výrobcrm zařízení, a to včetně nároku na nové verze firmware |  |  |
| **Přístupový přepínač 24 port včetně příslušenství** | 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 výrobcem zařízení, včetně nároku na nové verze firmware |  |  |
| **Přístupový přepínač 24 port PoE včetně příslušenství** | 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 výrobcem zařízení, včetně nároku na nové verze firmware |  |  |
| **Přístupový přepínač 48 port včetně příslušenství** | Základní parametry | L2+ přepínač v rackovém provedení max. 1U |  |  |
| Porty | min. 48x 10/100/1000Base-T RJ-45 porty + min. 4x 10 Gb/s SFP+ porty |  |  |
| Propustnost | přepínací kapacita min. 170 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 výrobcem zařízení, včetně nároku na nové verze firmware |  |  |
| **Kontrolér** | Základní funkce | Kontrolér je určený pro řízení a správu switchů a Wi-Fi přístupových bodů. Může být dodán jako samostatné HW zařízení nebo virtuální nebo softwarové řešení |  |  |
| Počet spravovaných zařízení | min. 150 access pointů a 30 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 sítích | 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 výrobcem zařízení, a to včetně nároku na nové verze firmware |  |  |
| **Vnitřní přístupový bod Wi-Fi 6 s příslušenstvím** | Základní funkce | Přístupový bod (AP) standardu Wi-Fi 6 včetně montážního materiálu na stěnu nebo strop |  |  |
| Frekvence | podpora Wi-Fi 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 2402 Mb/s v pásmu 5 GHz |  |  |
| Standardy | podpora 802.3at, 802.11n, 802.11ax, 802.1x včetně přiřazování do VLAN, podpora Wi-Fi kanálu s šířkou 160 MHz |  |  |
| 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-Wi-Fi rušení |  |  |
| Multi SSID | podpora vysílání min. 6 SSID (Wi-Fi 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 |  |  |
| Správa frekvenčního pásma | přechod klientů (roaming) mezi AP, automatické rozkládání zátěže mezi AP |  |  |
| Záruka | min. 60 měsíců poskytovaná výrobcem zařízení, včetně nároku na nové verze firmware |  |  |
| **Venkovní přístupový bod Wi-Fi 6 s příslušenstvím** | Frekvence | podpora Wi-Fi 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 2402 Mb/s v pásmu 5 GHz |  |  |
| Standardy | podpora 802.3at, 802.11n, 802.11ax, 802.1x včetně přiřazování do VLAN, podpora Wi-Fi kanálu s šířkou 160 MHz |  |  |
| 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-Wi-Fi rušení |  |  |
| Multi SSID | podpora vysílání min. 6 SSID (Wi-Fi sítí) v každém pásmu současně, podpora přiřazení každého SSID samostatné VLAN |  |  |
| Provedení | provedení pro venkovní montáž (outdoor) |  |  |
| 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 |  |  |
| Záruka | min. 60 měsíců poskytovaná výrobcem zařízení, včetně nároku na nové verze firmware |  |  |
| **Optické prvky** | Optický modul SFP+ 10 ks | Standards and Protocols IEEE 802.3ae, TCP/IP  Wave Length WDM  Power Supply 3.3V  Fiber Type 9/125um Single-Mode  Max. Cable Length 2 km  Data Rate 10 Gbps  Port Type LC |  |  |
| **Nasazení federovaného systému Eduroam** | Popis | připojení do federovaného systému Eduroam viz <https://www.eduroam.cz/cs/spravce/pripojovani> |  |  |
| **Systém pro řízení přístupu založený na IEEE 802.1X** | Popis | Instalace a konfigurace systému 802.1X pro zajištění autentizace uživatelů připojených přes LAN a Wi-Fi prostředky do počítačové sítě školy. Systém je založený na protokolu RADIUS a je integrovaný s Active Directory. |  |  |

| **Komodita C – Centrální logování, monitoring síťového provozu** | | | | |
| --- | --- | --- | --- | --- |
| **Část** | **Parametr** | **Popis povinného parametru** | **Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek** | **Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| **Systém pro sběr a správu logů a monitoring síťového provozu** | 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. |  |  |
| 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 přidávájí 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 přidávájí 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. |  |  |
| 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, zálohování a licence operačních systémů** | | | | |
| --- | --- | --- | --- | --- |
| **Část** | **Parametr** | **Popis povinného parametru** | **Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek** | **Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| **Server s příslušenstvím** | 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.  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. 6x 4 TB a v RAID6, 2x 1,92 TB DWPD 5 v RAID1 a 1x 240 GB SSD. Všechny disky musí být hot-plug, server obsahuje další min. 3 volné funkční sloty pro disky. |  |  |
| RAID řadič | Interní RAID řadič s min. 2 GB cache zálohovanou proti výpadku napájení. Podpora min. RAID1, RAID10, RAID5 a RAID6 bez nutnosti dokoupit další licence. Časově neomezená licence. |  |  |
| 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 | 4x 10 Gbps SFP+ s využitím OCP v. 3 |  |  |
| 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. 95 % 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. 440 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 garantovanou opravou nejpozději následující pracovní den po nahlášení závady |  |  |
| **Záložní zdroj s příslušenstvím – pro server** | 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 (záložní 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 |  |  |
| **Síťové úložiště s příslušenstvím pro ukládání záloh** | Provedení | Rack |  |  |
| Pozice pro disky | Min. 4 pozic pro HDD / SSD 3,5”, podpora Btrfs a ext4 souborových systémů |  |  |
| Operační paměť | Min. 2 GB DDR4 RAM |  |  |
| Rozšiřitelnost | Podpora připojení externích disků přes USB 3.0 |  |  |
| Výkon | Přenosová rychlost až 600MB/s při osazení 10Gb LAN |  |  |
| Komunikace LAN | Síťové protokoly CIFS, WebDAV, iSCSI, SSH, SNMP, http/s |  |  |
| Hot-swap | Disky vyměnitelné za chodu |  |  |
| Kapacita | Osazeno min. 4ks 4 TB HDD SATAIII/7200 RPM/256MB cache.  Disky se zárukou 36 měsíců, uvedené v seznamu kompatibilních disků výrobce zálohovacího zařízení. Velikost sektoru 512e |  |  |
| Konektivita | 2 x 1Gbps port a 1 x 10 Gbps |  |  |
| 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 |  |  |
| **Záložní zdroj s příslušenstvím – pro NAS** | 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 (záložní 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 |  |  |
| **Záložní zdroj s příslušenstvím – pro přepínače** | Provedení | do Racku, výška max. 1U, max. hloubka 24 cm |  |  |
| Výstupní výkon | min. 600 VA, 360 W |  |  |
| Rozmezí vstupního napětí | 165 ~ 271 Vac |  |  |
| Vstupní konektor | IEC C14 |  |  |
| Výstupní zásuvky | IEC C13 x 6 |  |  |
| Informační panel | LCD |  |  |
| Baterie | Uživatelsky vyměnitelné |  |  |
| Certifikace | CE, EAC, RCM |  |  |
| **Licence zálohovacího software** | Licence | Licence zálohovacího software pro min. 10 zálohovaných zařízení (nerozlišuje se mezi VM, fyzickým 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. |  |  |
| **Licence serverových operačních systémů** | Serverové licence | Serverové licence pro operační systém Windows Server v aktuální verzi. Licence musí pokrývat počet jader procesoru v dodaném serveru. Licence musí pokrývat provozování 4 virtuálních instancí serverového operačního systému. |  |  |
| **Přístupové serverové licence** | Klientské licence | Klientské licence pro operační systém Windows Server v aktuální verzi umožňující využívat těchto systémů uživatelům celkem na 100 zařízeních. |  |  |

| **Komodita E – Koncová zařízení** | | | | |
| --- | --- | --- | --- | --- |
| **Část** | **Parametr** | **Popis povinného parametru** | **Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek** | **Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| **Učitelský notebook** | CPU | Minimálně 12 jader, výkon dle Passmark minimálně 16800 bodů |  |  |
| RAM | Minimálně 16 GB DDR5 5600, možnost rozšíření na dva moduly |  |  |
| Pevný disk | Minimálně 512 GB SSD, typM.2, možnost přidání druhého disku |  |  |
| Grafika | Integrovaná |  |  |
| LCD | 16“ 16:10 |  |  |
| Bezdrátová komunikace | Wi-Fi® 6E, 802.11ax 2x2 + BT5.3 |  |  |
| Klávesnice | CZ, podsvícená |  |  |
| Bezpečnost | FHD IR kamera |  |  |
| Baterie | 45WH |  |  |
| OS | Plně kompatibilní s Windows 11 Pro |  |  |
| Záruka | * Minimálně 3 roky On-site |  |  |
| Odolnost | MIL-STD-810H military test passed |  |  |
| **Dobíjecí vozík** | Nabíjecí vozík pro notebooky a tablety, 30 nabíjecích stanic až 15,6", vč. USB, PDU, ventilátor | |  |  |
| 30 míst (3x10) 42 x 415 mm pro zařízení (rozteč mezi jednotlivými policemi minimálně 295 mm) | |  |  |
| 3x zásuvka na zadní straně (10 x bezpečnostní zdířky včetně spínače) | |  |  |
| Kompaktní pouzdro, mobilní – nainstalovaná kolečka | |  |  |
| Dvojité skládací přední a zadní dveře | |  |  |
| Tlakový uzávěr s otočnou rukojetí páky na předních a zadních dveřích, uzamykatelný | |  |  |
| Úhel otevření dveří 180 ° | |  |  |
| Dvoubodové zamykání (tyčový zámek) | |  |  |
| Včetně úchytů pro lepší mobilitu | |  |  |
| Bezpečnostní zásuvka (AC) se spínačem na boku | |  |  |
| **Žákovský notebook** | CPU | Minimálně 12 jader, výkon dle Passmark minimálně 17000 bodů |  |  |
| RAM | Minimálně 16 GB DDR5 5600 |  |  |
| Pevný disk | Minimálně 512 GB SSD, typM.2 G4 |  |  |
| Grafika | Integrovaná |  |  |
| LCD | 16“ 16:10 |  |  |
| Bezdrátová komunikace | LAN\_2X2AX\_6E+BT |  |  |
| Klávesnice | CZ, podsvícená |  |  |
| Bezpečnost | FHD IR kamera |  |  |
| Baterie | 45WH |  |  |
| OS | Plně kompatibilní s Windows 11 Pro |  |  |
| Záruka | Minimálně 3 roky On-site |  |  |
| Odolnost | MIL-STD-810H Military Test Passed |  |  |

# Požadavky na instalační a implementační práce

**Komodita B – Zabezpečení LAN a Wi-Fi**

* 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 Wi-Fi bude založena na řešení s centrální správou prováděnou hardwarovým nebo virtuálním kontrolerem (řadičem). Hardwarový nebo virtuální kontroler bude konfigurován v režimu vysoké dostupnosti a zajistí automatické rozložení zátěže klientů, roaming mezi spravovanými přístupovými body a automatické ladění kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení.
* Umístění pořízených AP bude provedeno na základě provedené analýzy pokrytí signálem pro zajištění konzistentní Wi-Fi služby v pokrytých prostorách. Provedení analýzy bude součástí projektu.
* 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 Wi-Fi sítě bude realizováno na stejném principu jako LAN (tj. protokol 802.1x + radius). Wi-Fi bude nabízet více SSID (učitelé, žáci, Guest), které budou obsluhovány samostatnými VLAN a budou napojeny na raduis servery. Učitelé a žáci budou prostřednictvím radius serveru ověřováni v adresářové 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 Wi-Fi), kde bude realizován tzv. captive portál zajišťující webovou autentizaci hostů pomocí přidělených účtů nebo za pomoci před-generovaných číselných kupónů. Preferován bude captive portál firewallu s tzv. lobby přístupem pro správu a generování účtů/kupónů ne-technickou osobou.
* 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 Wi-Fi 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 – např. vytvoření informační webové stránky, zajištění technického kontaktu apod. Zapojení do systému EDUROAM zajistí národní i mezinárodní mobilitu žáků a učitelů.

**Komodita C – Centrální logování, monitoring síťového provozu**

* 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. Další funkcionalitou bude plnohodnotná práce se síťovými toky, jejich zpracování a archivace. Nástroje systému budou umožňovat i analytickou práci s přijímanými toky a to i zpětně.
* 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.

**Komodita D – Server, diskové pole, UPS, zálohování a licence operačních systémů**

* V rámci projektu bude pořízen 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 projektu. Zároveň, při přenosu virtuálních serverů a služeb na nový server bude také proveden upgrade všech operačních systémů na nejnovější dostupné verze.
* Server bude mít zajištěnou záruku v místě instalace s garantovanou opravou následující pracovní den po nahlášení, a to přímo od výrobce serveru, v délce 60 měsíců.
* Ochranou nově pořízených technologií vůči výpadku elektrického proudu bude UPS, která bude také pořízena v rámci projektu.
* 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.
* Požadované 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).

**Komodita E – Koncová zařízení**

* Součástí komodity je dodávka, instalace a konfigurace koncových zařízení potřebných pro vedení výuky.

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:

|  |
| --- |
| Komodita B – Zabezpečení LAN a Wi-Fi |
| 1. Analýza stávajícího síťového prostředí a návrh nového architektury LAN i Wi-Fi 2. Implementace pořízených technologií 3. Provedení segmentace LAN – VLAN, adresování, směrování/routování 4. Zavedení IPv6 pro přístup k internetovým zdrojům publikovaným na IPv6 adresách 5. Zavedení IPv6 pro veškeré publikované služby z interních či externích prostředků. Včetně zajištění jednání a řízení 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. 6. Zabezpečení komunikace publikovaných služeb pomocí nabízeného certifikátu. 7. Zavedení DNSSEC pro interní DNS služby i zabezpečení domén škol. 8. Návrh a implementace 802.1X pro kabelovou LAN i Wi-Fi včetně uživatelské dokumentace pro konfigurace obvyklých zařízení a jejich systémů-PC, notebooky, chytré telefony, tablety, tiskárny-Windows, Linux, MacOS, Android, IOS, embedded systémy periferií 9. Návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) pro školy 10. Vybudování VPN pro vzdálený přístup uživatelů LAN na bázi webového portálu 11. Respektování min. 3 různých skupinu uživatelů (učitelé, studenti, hosté) v návrzích a implementaci bezpečnostních a ostatních politik 12. Implementace portálu pro registraci a řízení přístupů hostů – tzv. captive portál 13. Zapojení školy do federovaného systému eduroam 14. Zajištění ostatních nezbytných činností pro naplnění Standardu konektivity 15. Návrh a provedení akceptačních testů, musí zahrnovat testy propustnosti LAN a pokrytí Wi-Fi |
| Komodita C – Centrální logování, monitoring síťového provozu |
| 1. Návrh a implementace systému pro centrální logování pro naplnění požadavků Standardu konektivity, především, ale nejen:    * monitoring a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu  k vnitřnímu zařízení (ve spolupráci s firewallem)    * logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel, a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)    * monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) -RFC3954 nebo ekvivalent (např. netflow) – systém pro monitorování a sběr provozně-lokačních údajů minimálně na úrovni rozhraní WAN, ideálně i LAN) a to bez negativních vlivů na zátěž  a propustnost zařízeni 2. Provedení souvisejících konfigurací monitorovaných systémů 3. Návrh a provedení akceptačních testů, musí zahrnovat ověření logování veškerých požadovaných uživatelů a správnost přiřazení identit uživatelů logovaným údajům |
| Komodita D – Server, diskové pole, UPS, zálohování a licence operačních systémů |
| 1. Dodávka a kompletní zprovoznění nabízených komponent včetně potřebných konfiguračních služeb 2. U upgradů operačních systémů nabízených zařízení není požadováno provedení instalace  a aktivace upgrade. Uvedené činnosti provede zadavatel vlastními silami dle dodavatelem připraveného vzorku a dodavatelem poskytnuté dokumentace |
| Komodita E – Koncová zařízení |
| 1. Dodávka a kompletní zprovoznění nabízených zařízení včetně potřebných montážních prací a instalace obslužných programů, které jsou součástí dodávky |

V rámci implementace předmětu plnění dodavatel realizuje pro všechny nabízené komodity následující služby:

* 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 Practice) 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 Wi-Fi-připojení zařízení vč. podrobných uživatelských postupů pro Wi-Fi 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 v rozsahu dle kapitoly 2.4.
* 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 8 hodin do 17 hodin.
* Provedení akceptačních testů.
* Předání do plného provozu.

Činnosti omezující práci uživatelů musí být prováděny mimo běžnou pracovní dobu, tj. mimo pracovní dny 7–15 hod.

## 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.

## 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 nesplňuje. Škola zajistí navýšení konektivity u stávajícího dodavatele, nebo uzavře smlouvu s novým dodavatelem na vyšší rychlost, tím bude tento parametr naplněn. |
| Vlastní nebo poskytovatelem přidělené veřejné IPv4 adresy. | Ano | Tento parametr škola v současné době nesplňuje. Škola uzavře s poskytovatelem smlouvu o přidělení veřejné IPv4 adresy. |
| 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 nesplňuje. Budou pořízeny aktivní prvky s podporou IPv6 a ve spolupráci s poskytovatelem internetu provedena konfigurace, tím bude parametr naplněn. |
| Konektivita školy k veřejnému internetu (WAN) - doporučené parametry | | |
| Symetrické připojení (zajištění konektivity) bez agregace a omezení. | Ano | Tento parametr škola v současné době nesplňuje. Bude uzavřena nová smlouva s ISP, tím bude parametr naplněn. |
| 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". 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 kupujícího, pro něž prodávající písemně poskytne potřebné požadavky na konfigurace. Prodávající proto v rámci svého plnění musí postupovat tak, aby tyto třetí strany měly odpovídající časový prostor v rámci jejich součinnosti zajišťované kupujícím tyto konfigurace provést (nastavit) a prodávající pak mohl pro kupujícího zajistit komplexní výstupy naplnění standardu konektivity, které následně kupujícímu poslouží jako výstup pro prokázání naplnění požadavků jím realizovaným projektem.

# Harmonogram plnění

Kupující požaduje dodat a implementovat technologie v termínu plnění stanoveném v návrhu kupní smlouvy. Dodavatel se v rámci plnění zavazuje dodržet harmonogram v níže uvedené podobě. Údaj D značí datum nabytí účinnosti kupní smlouvy. Čísla značí počet kalendářních dnů.

Dodavatel může dle svého uvážení výše uvedené maximální lhůty trvání zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb.

| Aktivita | Začátek | Termín splnění |
| --- | --- | --- |
| Účinnost smlouvy | D | D |
| Zahájení projektu – úvodní projektová schůzka | D | D+5 |
| Předimplementační analýza – zpracování | D+5 | D+20 |
| Předimplementační analýza – připomínkové řízení, schválení | D+20 | D+27 |
| Prováděcí dokumentace – zpracování | D+27 | D+35 |
| Prováděcí dokumentace – připomínkové řízení, schválení | D+35 | D+40 |
| Realizace předmětu plnění | D+40 | D+120 |
| Školení administrátorů | D+120 | D+140 |
| Zkušební provoz | D+120 | D+140 |
| Akceptační testy | D+120 | D+150 |
| Zahájení ostrého provozu | D+150 | - |