



Příloha 1: Technická specifikace

1. Popis výchozího stavu

1.1. Základní škola a mateřská škola Tři Sekery

- (1) Základní škola Tři Sekery tvoří komplex dvou budov, které jsou spojeny spojovací chodbou. V současné době navštěvuje školu cca. 48 žáků.
- (2) Realizace projektu bude probíhat ve všech využívaných prostorách budovy školy.
- (3) Současný stav ICT školy neodpovídá Standardu konektivity škol (dále jen Standard konektivity), a současným nárokům na výkon, bezpečnost a centralizovanou správu počítačové sítě. Počítačová síť byla budována postupně, staří a technické úroveň používaných prvků se liší. Síťové pokrytí – drátové i bezdrátové – bylo v jednotlivých etapách realizováno na pokrytí aktuálních potřeb a s ohledem na omezené finanční možnosti, bez rezerv pro budoucí rozvoj. Část prvků je technicky i morálně zastaralých a výrobci nepodporovaných. Chybí provázanost jednotlivých částí. Chybějící systém správy identit neumožňuje automatizované udržování individuálních elektronických identit pro všechny uživatele sítě (žáci i učitelé) a následné automatické uplatňování politik pro řízení, monitorování a logování síťové a internetové komunikace. Absence možnosti 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.
- (4) Kabelové rozvody v budovách jsou provedeny kabely různých kategorií. Kabeláž není plně strukturovaná a nevyhovuje jednotnému standardu. Pokrytí všech budov metalickými rozvody je nedostatečné a neumožňuje připojovat do sítě další zařízení (koncová zařízení, IoT a bezpečnostní prvky (kamery apod.)) a síť rozvíjet např. doplňováním WiFi přístupových bodů. Nedostatek přípojných míst je řešen „rozbočováním“ sítě malými přepínači bez managementu, jejichž použití dále komplikuje správu celé sítě a snižuje její robustnost, stabilitu a bezpečnost.
- (5) Internetové připojení v současnosti zajišťuje společnost O2 prostřednictvím spoje o rychlosti 50/50 Mbps. Rychlost připojení tak odpovídá požadavku Standardu konektivity škol – 45 Mbps (48 žáků x 0,25 Mbps).
- (6) Škola nemá přiděleny veřejné IP adresy IPv4 ani IPv6. Škola nemá v současné době validující DNSSEC resolver na straně školy, neprovádí pokročilý monitoring provozu.
- (7) Škola provozuje spojení Wifi s částečným pokrytím. Slouží pouze pro potřeby zaměstnanců školy. Přístup k síti je zabezpečený sdíleným heslem. Síť není centrálně spravovaná a použité prvky nedisponují podporou dostatečného počtu VLAN a jejich automatického přidělování pro segmentaci sítě školy. Prvky nepodporují aktuální bezpečnostní standardy (WPA3 apod.) ani pokročilé funkce optimalizace rádiového provozu a obsluhy připojených klientů.
- (8) Zabezpečení přístupu k internetu využívá pouze NAT na hraničním prvku – routeru. Nejsou využívány pokročilé bezpečnostní funkce např. URL filtrace, antivirová kontrolou a detekce průniků.
- (9) Škola nedisponuje žádným zálohovacím systémem.
- (10) Škola nedisponuje centrální databází uživatelských identit Active Directory. Škola neprovozuje žádný systém pro automatizovanou správu a správu souvisejících oprávnění – IdM (Identity Management).
- (11) Přístup do počítačů (resp. operačních systémů) je řízen převážně sdílenými lokálními uživatelskými účty.
- (12) Hlavní softwarovou platformou uživatelských počítačů jsou operační systémy společnosti Microsoft. Na koncových počítačích učitelů i žáků jsou používány převážně operační systémy Windows 10 a vyšší bez podpory domény Active Directory. Škola provozuje cca. 30 počítačů. Správa životního cyklu operačních systémů a aplikačního vybavení se provádí manuálně.
- (13) Škola využívá cloudové služby Microsoft 365 A3.



2. Popis cílového stavu a specifikace předmětu plnění

2.1. Základní požadavky na technické řešení

- (1) V rámci projektu bude maximalizováno využití prostředků pořízených v předchozích projektech tam, kde je to technicky, provozně a z pohledu bezpečnosti vhodné a možné.
- (2) Cílem projektu je zvýšení bezpečnosti a související modernizace IT infrastruktury, aby implementací projektu byly naplněny Standardy konektivity škol¹ (dále jen Standard konektivity) a rozšířena funkčnosti ICT prostředí zapojených škol.
- (3) Je požadováno řešení zachovávající a rozvíjející současné softwarové platformy Microsoft pro zachování kompatibility se stávajícími systémy a aplikacemi. Přechod na jinou platformu by způsobil uživatelské a provozní potíže.
- (4) Je požadována unifikace jednotlivých komodit (tj. jejich realizace stejnými prostředky) pro všechny části z důvodu jednotné správy celého prostředí a odpovídající minimalizace provozních nákladů.
- (5) Pokud prodávající (dále jen jako „dodavatel“) vyžaduje využití konkrétních softwarových produktů a jím zvolený přístup k realizaci zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.
- (6) Pokud dodavatelem nabízené řešení vyžaduje komponenty či služby neobsažené v požadavcích zadání, zahrne dodavatel do své ceny všechny náklady na jejich pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu, přičemž nesmí překročit ceny za pořízení a provoz v rámci příslušných částí stanovené v Zadávací dokumentaci.
- (7) Kupující (dále též jako „zadavatel“) z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů vyžaduje využití stávajících prostředků a používaných technologií. V případě, že dodavatel vyžaduje ve svém řešení stejné nebo podobné funkce, jaké poskytují stávající prostředky a technologie, je povinen využít nebo vhodným způsobem rozšířit stávající prostředky.
- (8) Veškeré produkty, které dodavatel dodává v rámci plnění zadavatel, musí splňovat následující podmínky a dodavatel splnění těchto podmínek potvrdí samostatným čestným prohlášením, které doloží do 15 dnů po podpisu smlouvy:
 - (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.

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

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

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

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



2.2. Specifické požadavky na technické řešení komodit

(1) Zabezpečení LAN a Wifi

- (a) Pro hosty a externí uživatele bude zřízena samostatná VLAN (Guest VLAN), které bude komunikačně oddělena od vnitřních sítí organizace
- (b) Architektura WiFi bude založena na řešení s centrální správou prováděnou HW kontrolerem, který 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.
- (c) Umístění pořízených AP bude provedeno na základě provedené analýzy pokrytí signálem pro zajištění konzistentní WiFi služby v pokrytých prostorách. Provedení analýzy bude součástí projektu.

(2) Centrální logování

- (a) Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací. Řešení umožní správu z jedné grafické konzole, přístupné nativně skrze portál 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.

(3) Koncová zařízení a licence operačních systémů

- (a) Požadované licence operačních systémů musí umožnit využití implementovaných funkcionalit serverových řešení.
- (b) 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.

(4) Interaktivní technika

- (a) Součástí komodity je dodávka, instalace a konfigurace interaktivních panelů pro vedení výuky.
- (b) Interaktivní dotykový panel, multitdyk 40 prstů, rozlišení panelu 4K, vlastní operační systém
- (c) Elektrický pojezdový systém panelu s křídly s rozsahem zvedání 800 – 1750 mm.

(5) Rozvody LAN

- (a) Rozvody LAN budou vybudovány jako hvězdicovité, tj. distribuční přepínače (popř. sestavy/stohy přepínačů v datovém rozvaděči) budou přímo napojeny na centrální přepínač školy tak, aby na centrálním přepínači mohl být monitorován veškerý síťový provoz školy s výjimkou peer-to-peer komunikací v rámci distribučních přepínačů.

2.3. Implementační služby

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

- (a) Zpracování prováděcí dokumentace, podle které bude dodavatel řešení implementovat. Prováděcí dokumentace musí být před zahájením implementace výslovně schválena zadavatelem.
- (b) Dodávka a implementace předmětu plnění dle schválené prováděcí dokumentace včetně technické podpory.
- (c) Zajištění projektového vedení realizace předmětu plnění.
- (d) Zajištění zkušebního provozu infrastruktury v délce minimálně 2 týdnů včetně technické podpory specialistů na dané zařízení/službu s dostupností maximálně do 2 hodin na místě realizace od nahlášení požadavku v pracovní den v době od 8h do 17h.
- (e) Provedení akceptačních testů.
- (f) Předání do plného provozu.



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

Zadavatel dále požaduje provést minimálně následující implementační služby na dodaných komponentech a zařízeních. Dodavatel je dále povinen zahrnout do nabídky veškeré další činnosti a prostředky, které jsou nezbytné pro provedení díla v rozsahu doporučeném výrobcem a dle tzv. nejlepších praktik, i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné.

Zabezpečení LAN a Wifi
a) Analýza stávajícího síťového prostředí a návrh nové architektury LAN i WiFi b) Implementace pořízených technologií c) Provedení segmentace LAN – VLAN, adresování, směrování/routování d) Návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) pro školy e) Respektování min. 3 různých skupin uživatelů (učitelé, studenti, hosté) v návrzích a implementaci bezpečnostních a ostatních politik f) Zajištění ostatních nezbytných činností pro naplnění Standardu konektivity g) Návrh a provedení akceptačních testů, musí zahrnovat testy propustnosti LAN a pokrytí WiFi
Centrální logování
a) Návrh a implementace systému pro centrální logování pro naplnění požadavků Standardu konektivity, především, ale nejen: <ul style="list-style-type: none">• 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.) b) Provedení souvisejících konfigurací monitorovaných systémů c) Návrh a provedení akceptačních testů, musí zahrnovat ověření logování veškerých požadovaných uživatelů a správnost přiřazení identit uživatelů logovaným údajům
Koncová zařízení a licence operačních systémů
a) Dodávka a kompletní zprovoznění nabízených komponent včetně potřebných konfiguračních služeb
Interaktivní a výuková technika
a) Dodávka a kompletní zprovoznění nabízených zařízení včetně potřebných montážních prací a instalace obslužných programů, které jsou součástí dodávky

(3) Akceptační testy musí pro všechny komodity vždy zahrnovat minimálně prokázání kompletnosti dodávky a požadované funkčnosti. Prokázání naplnění požadavků poskytne dodavatel v písemné formě vhodné jako příloha k Závěrečné zprávě o realizaci projektu.

(4) Náklady na provedení implementačních služeb musí být zahrnuty v nabídkové ceně k položce (komoditě), ke které se vztahují a nelze je vyčíslit zvlášť.

2.4. Školení

(1) Dodavatel provede pro každou komoditu odborné školení na obsluhu a práci s dodanými zařízeními, a to minimálně v rozsahu provozní dokumentace.

(2) Školení bude pokrývat všechna zařízení a systémy všech komodit, dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu:

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



- (3) Školení dále zajistí seznámení pracovníků zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.
- (4) Minimální rozsah školení pro každou komoditu jsou 2 hodin



Spolufinancováno
Evropskou unií

Ministerstvo životního prostředí