Technická specifikace - popis

„Vnitřní konektivita školy“
Zadavatel: Střední škola obchodní a Vyšší odborná škola, České Budějovice, Husova 9, IČ: 00510874

1. Popis výchozího stavu

(1) Aktuální Wi-Fi síť je tvořena 1 přípojným bodem, který pokrývá jen část prostorů. Pro ověření uživatelů se používá sdílené heslo.

(2) Lokální klimatizovaná serverovna je umístěna v 1. NP, zdejší racková skříň bude sloužit i pro nový server.

(3) Zálohování a obnova dat je řešeno pomocí externích disků.

2. Popis cílového stavu a specifikace předmětu plnění

2.1. Základní požadavky na technické řešení

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

	Komodita
A	Vytvoření zabezpečené WiFi sítě
B	Zabezpečení stávající konektivity
C	Systém zálohování a obnovy dat - server

(2) 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.

(3) Pokud dodavatel vyžaduje využití konkrétních softwarových produktů a jím zvolený přístup k realizaci zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.

(4) Zadavatel z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů vyžaduje využití stávajících prostředků a používaných technologií. V případě, že dodavatel vyžaduje ve svém řešení stejné nebo podobné funkce, jaké poskytují stávající prostředky a technologie, je povinen využít nebo vhodným způsobem rozšířit stávající prostředky.

(5) Zadavatel zabezpečí konektivitu připojení k síti internet v souladu s požadavky Standardu konektivity.

(6) Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky a dodavatel splnění těchto podmínek potvrdí samostatným čestným prohlášením:

(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.

(7) Veškerá dokumentace dodávaná v rámci veřejné zakázky, musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. MS Office, PDF) používaných zadavatelem na datovém nosiči a 1x v papírové formě. Papírová forma bude logicky a věcně strukturovaná, bude připravena pro použití (např. provozní dokumentace ve formě vhodné pro použití administrátory v serverovně). Struktura i forma dokumentace musí být před předáním předána ke kontrole a výslovně schválena zadavatelem.

2.2. Specifické požadavky na technické řešení

(a) Bezpečnost, řízení přístupů

(i) Bude implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby s využitím technologie 802.1X.

(b) 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.

(c) Řízení provoz v LAN bude realizováno vytvořením VLAN (802.1Q), segmentací sítě s routováním (přepínáním) provozu mezi VLAN na úrovni centrálního přepínače s nastavitelnými ACL. Pro řízení provozu na úrovni kvality služeb bude k dispozici technologie QoS (Quality of Services). Pro zajištění vysoké dostupnosti služeb budou klíčové aktivní prvky propojeny duálními trasami s automatickým rozkládáním zátěže a převzetím služeb v případě výpadku jedné trasy.

(d) Architektura WiFi je a zůstane založena na centralizovaném řešení s centrální správou prováděnou centrálním kontrolerem (řadičem) zajišťujícím automatické rozložení zátěže klientů, roaming mezi spravovanými access pointy a automatické ladění kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení.

(e) Umístění pořízených AP bude provedeno na základě provedené analýzy pokrytí signálem pro zajištění konzistentní WiFi služby v pokrytých učebnách. Provedení analýzy bude součástí projektu.

(f) Ověřování přístupu do LAN bude realizováno protokolem 802.1X vůči adresářové službě prostřednictvím protokolů radius a P/EAP. Zařízení musí vybavena tzv.

suplikantem - softwarovou komponentou, která dokáže předávat ověřovací požadavky síťovým prvkům, které tyto požadavky ověří vůči adresářové služby. Pro ověření zařízení bez suplikantů (např. starší tiskárny, zařízení na bázi jednoduchých operačních systémů či firmware apod.) bude použit jiný 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.

(g) Ověřování přístupu do WiFi sítě bude realizováno na stejném principu jako LAN (tj. protokol 802.1X + radius). Wifi bude nabízet min. 3 SSID (učitelé, žáci, Guest), které budou obsluhovány samostatnými VLAN a budou napojeny na různé radius servery. Učitelé a žáci budou prostřednictvím radius serveru ověřováni v adresářové služby. Zabezpečení vnitřních sítí (BSSID) školy bude provedeno dle 802.1i, tedy - WPA2 s AES šifrováním a konfigurováno shodně pro obě frekvenční pásma. Výjimkou bude síť určená výhradně pro hosty (Guest WiFi), kde bude realizován tzv. captive portál zajišťující webovou autentizaci hostů pomocí přidělených účtů nebo za pomoci předgenerovaných číselných kupónů. Preferován bude captive portál firewallu s tzv. lobby přístupem pro správu a generování účtů/kupónů ne-technickou osobou.

(h) Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací – může se jednat o jediné zařízení, softwarový nástroj či appliance nebo o řešení složené z více samostatných a vzájemně kompatibilních komponent. Preferované bude takové řešení, které umožní správu z jedné grafické konzole integrovaných komponent, ideálně přístupné nativně skrze https bez nutnosti instalace klienta. Další preferencí bude ukládání všech informací 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).

(i) Veškeré dále požadované informace si bude systém automatiky 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.

(j) 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 na straně firewallu za pomoci jeho SSO agentů či logů 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.

(k) Kombinací požadavků zákona o uchování informací v elektronické komunikaci spolu s požadavky Standardu konektivity škol a praktického pohledu na možné časové prodlení mezi vznikem incidentu a jeho vyšetřováním je definováno, že monitorovací a logovací systém bude umožňovat retenci dat min. 180 dnů. Na tento rozsah retence

musí být dostatečně dimenzován, především z hlediska diskové kapacity, RAM i CPU, tak aby nedocházelo k výkonovým ani kapacitním problémům a systém měl dostatečnou rezervu pro očekávatelný budoucí nárůst informací a jejich zdrojů.

(l) Pro provoz veškerých pořízených systémů a aplikací bude pořízen jeden server vybavený rychlým interním úložištěm s vysokou kapacitou. Hardware serveru bude virtualizován a na serveru bude možno provozovat několik virtuálních serverů. Server bud připojen do sítě duální optickou linkou 2x 1 Gb. Pořízený server musí být výrobcem určen pro provoz v běžném, neklimatizovaném prostředí do teploty 35 stupňů Celsia.

(m) Pro zálohování bude v rámci projektu pořízeno síťové uložiště NAS s dostatečnou kapacitou pro ukládání provozních záloh a archivů logů monitorovacího a logovacího systému. Zálohování bude řízeno pokročilým zálohovacím software, který bude prostřednictvím virtualizačního hypervizoru zálohovat všechny virtuální servery. Sítové úložiště NAS bude kvůli bezpečnému oddělení záloh od produkčních dat umístěno mimo místnost serveru - optimálně zabezpečené (uzamykané) místnosti v jiné budově.

(n) Provozní zabezpečení bude tvořeno souborem non-IT technologií, které zajistí optimální podmínky pro spolehlivý chod technologií – především serveru:

(i) Záložní zdroj napájení UPS zajistí chod serveru při výpadku napájení

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

(o) Pro zajištění bezpečnosti a možnosti řízení provozu v síti a zajištění prokazatelného monitoringu, logování a auditu interního i externího síťového provozu bude vybudována centrální databáze identit na bázi adresářové služby. Adresářová služby umožní ukládání a přehlednou správu identit (účtů včetně metadat) učitelů, žáků i externích subjektů, ale i technických prostředků – serverů, tiskáren, pracovních stanic apod. Adresářová služba bude poskytovat službu LDAP a umožní snadné napojení autentizačních mechanismů a protokolů – radius, agent firewallu a dalších. Adresářová služba zajistí ověřování uživatelů pro účely jejich autorizace k přístupu k síťovým prostředkům (LAN, Internet atd.) i výpočetním zdrojům (pracovní stanice, tiskárny, sdílené složky atd.). Technické provedení bude založeno na řadiči adresářové služby. Řadič bude provozován ve virtuálním prostředí a bude pravidelně automaticky zálohován. Součástí řadiče budou základní síťové služby – DNS, DHCP. Ověřování identit musí být dostupné i systémům, které přímo nepodporují LDAP nebo jiný protokol adresářové služby. Součástí projektu bude proto i vybudování tzv. zprostředkovatelů identit, které umožní ověřování i jinými protokoly. Technicky půjde o softwarové komponenty transformující požadavky na ověření identity do formátu akceptovaného adresářovou službou.

2.3. Implementační služby

(1) V rámci implementace předmětu plnění dodavatel realizuje pro všechny nabízené komodity uvedené v kapitole 2.6. – komodity A až C – následující služby:

(a) Provedení předimplementační analýzy (včetně plánovaných změn v konfiguraci současné infrastruktury) a zpracování detailního finálního popisu cílového stavu a postupu implementace. Výstupem bude prováděcí dokumentace, podle které bude dodavatel řešení implementovat. Prováděcí dokumentace musí být před zahájením

implementace výslovně schválena zadavatelem. Prováděcí dokumentace musí respektovat a využívat osvědčené praktiky (tzv. Best Practice) a doporučení výrobců nabízených technologií.

(b) Dodávka a implementace předmětu plnění dle schválené prováděcí dokumentace včetně technické podpory.

(c) Zajištění projektového vedení realizace předmětu plnění.

(d) Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení a popisu činností běžné údržby a činností pro spolehlivé zajištění provozu.

(e) Zpracování dokumentu Zásady využívání ICT a přístupu k síti dle Standardu konektivity pro začlenění do vnitřních předpisů školy.

(f) Zpracování materiálů pro školení a provedení školení v rozsahu dle kapitoly 2.4.

(g) Provedení akceptačních testů.

(h) Předání do plného provozu.

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

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

a) Návrh a kompletní implementace serverové virtualizační platformy

b) Implementace pořízených technologií

c) Návrh vhodné struktury Active Directory a její vybudování

d) Návrh a realizace zálohovacího řešení

e) Implementace automatické odstávky a najetí serveru v případě výpadku a obnovení dodávky elektrické energie

f) Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy

a) Analýza stávajícího síťového prostředí a návrh nového architektury LAN i WiFi

b) Implementace pořízených technologií

c) Provedení segmentace LAN – VLAN, adresování, routování

d) Zavedení IPv6 pro přístup k internetovým zdrojům publikovaným na IPv6 adresách

e) Zavedení IPv6 pro veškeré publikované služby školy z interních či externích prostředků. Včetně zajištění jednání a řízení změn u externích poskytovatelů služeb. Jde zejména o služby hostování domény http://www.sso.cz/.cz, DNS, e-mail, web školy

f) Zavedení DNSSEC pro interní DNS služby i zabezpečení domény http://www.sso.cz/

g) Návrh a implementace 802.1X pro kabelovou LAN i WiFi včetně uživatelské dokumentace pro konfigurace obvyklých zařízení a jejich systémů - PC, notebooky, chytré telefony, tablety, tiskárny - Windows, Linux, MacOS, Android, IOS, embedded systémy periferií

h) Návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) pro školu

i) Vybudování VPN pro vzdálený přístup uživatelů LAN na bázi webového portálu

j) Respektování min. 3 různých skupinu uživatelů (učitelé, studenti, hosté) v návrzích a implementaci bezpečnostních a ostatních politik

k) Implementace portálu pro registraci a řízení přístupů hostů – tzv. captive portál

l) Zajištění ostatních nezbytných činností pro naplnění Standardu konektivity

m) 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

n) Provedení souvisejících konfigurací monitorovaných systémů

(4) Akceptační testy musí pro všechny komodity vždy zahrnovat minimálně prokázání kompletnosti dodávky a požadované funkčnosti. Návrh vhodných akceptačních kritérií bude součástí nabídky, zadavatel může v průběhu zpracování Předimplementační analýzy provést jejich upřesnění či rozšíření. Povinným akceptačním kritériem bude prokázání naplnění požadavků Standardu konektivity dle manuálu uveřejněného na http://www.strukturalni-fondy.cz/cs/Microsites/IROP/Novinky/Zverejneni-doporucujiciho-manualu-k-postupum-pri-prokazani-a-kontrole včetně úspěšného provedení a doložení testu na https://www.standardkonektivity.cz/. Prokázání naplnění požadavků poskytne dodavatel v písemné formě vhodné jako příloha k Závěrečné zprávě o realizaci projektu.

(5) 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 hodiny, není-li uvedeno jinak. Školení bude probíhat v sídle zadavatele. Předpokládá se účast max. 3 osob.

2.5. Harmonogram projektu

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

Aktivita	Začátek	Termín
Účinnost smlouvy	D	D
Zahájení projektu – úvodní projektová schůzka	D	D+7
Zpracování předimplementační analýzy a prováděcí dokumentace	D+7	D+20
Realizace předmětu plnění	D+20	D+34
Školení	D+34	D+35
Akceptační testy	D+35	D+38
Rezerva projektu	D+38	D+45
Zahájení ostrého provozu	D+45	-

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

(3) Maximální lhůty trvání nesmí dodavatel při tvorbě detailního harmonogramu prodloužit.

(4) Dodavatel uvede závazný harmonogram plnění ve své nabídce a zároveň v návrhu smlouvy.

(5) Dodavatel uvede potřebnou součinnost zadavatele pro splnění harmonogramu plnění ve své nabídce. Součinnost zadavatele ovlivňuje předpokládané termíny plnění dle harmonogramu, o termín poskytnutí součinnosti se posouvá termín realizace dané aktivity.

(6) Nejpozdější termín pro zahájení ostrého provozu a ukončení implementační fáze projektu je uvedena v Zadávací dokumentaci.

(7) Zadavatel zabezpečí připravenost prostorů realizace projektu.

3. Záruky a servisní podmínky

3.1. Požadavky na záruky a servisní podmínky

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

(2) Z důvodu zajištění udržitelnosti projektu po dobu 60-ti měsíců požaduje zadavatel poskytnutí záruky pro servery (A), firewall (B) na 60 měsíců při zachování ostatních parametrů původní záruky (rychlost opravy, rozsah aktualizací firmware apod.).

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

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

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

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

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

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

(9) Pro hlášení servisní požadavků zajistí dodavatel zhotoviteli přístup ke svému helpdeskovému systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení.