|  |
| --- |
| **Příloha č. 1: Technická specifikace** |

## Popis výchozího stavu

Současná ICT infrastruktura ZŠ a ZUŠ Petřvald, Školní 246, příspěvková organizace, (dále jen škola nebo ZŠ) je tvořena mixem starších technologií pořízených a implementovaných v uplynulých letech. Jedná se především o 1 ks fyzického serveru, router, síťové přepínače, WIFI AP, datové rozvody a koncové stanice. Aktuálně je ve struktuře ZŠ 73 členů učitelského sboru a administrativy a 830 žáků.

### Síťová infrastruktura

* + - * 1. **WAN** – základní škola je připojena do internetu přes poskytovatele TECHCOM s rychlostí stahování 50MBit/s a rychlostí odesílání 50MBit/s. Připojení je realizováno pomocí veřejné IP adresy 109.231.152.90 a škola využívá vlastní Firewall značky MIKROTIK, model CloudCore CCR1009-7G-1C, neobsahuje „chytré funkce“ next-generation firewallu.
        2. **LAN** – pro rozvody vnitřní sítě jsou použity switche, které jsou od různých výrobců a pracují s rychlostí 100Mbit až 1000Mbit. Část switchů je bez administrace, nejsou napojené na UPS. Přepínače jsou umístěny v rozvaděčích. Rozvody místní sítě mají charakter strukturované kabeláže. Počet rozvaděčů v budově je 10. Technologie automatického přidělování adres IPV4 je nasazena s Windows DHCP serverem na Virtuálním stroji. Technologie automatického přidělování IPV6 adres není nasazena. DNSSEC v interní síti také není nasazen. Škola není zapojena do projektu Fenix ani Eduroam.
        3. **WIFI** – škola má pokrytí bezdrátovým Wifi signálem. Použitý model pro bezdrátové body jsou Unifi UAP-AC-Pro. Všechny AP mají centrální management Unifi, instalován jako službu na jednom z virtuálních serverů. Managment je také dostupný pro místního IT správce. Některé Unifi AP nejsou napájeny z POE switche. Počet použitých AP je cca 26. Pokrytí školy pro případné evropské projekty není dostatečné.
        4. **WEB** – stránky školy jsou provozovány na adrese www.zsazuspetrvald.cz, doména je zabezpečena technologií HTTPS s důvěryhodným certifikátem. Technologie zabezpečení webových stránek DNSSEC není aktivní. Veřejná IPV6 adresa na webových stránkách není nasazena.
        5. **EMAIL** – doména školy má koncovku druhého řádu – zsazuspetrvald.cz a je shodná s doménou webových stránek. MX záznamy ukazují, že poštovní služby jsou provozovány na Microsoft Office 365 pro školy.

### Serverová infrastruktura

* + - * 1. **Virtualizace serverů** – aktuálně je nasazena virtualizace na technologii VMware vSphere ve verzi 6.0.0, která již není supportována ze strany výrobce.
        2. **Fyzické servery** – jeden fyzický server HPE Proliant ML150 Gen9 je hostitelem výše zmíněné virtualizace. Server je již po záruce. Další fyzické servery nejsou provozovány. Místo pro servery je v počítačové učebně, která je klimatizována. Server je uzamčen v RACKu a je připojen k záložnímu zdroji napájení UPS APC 750VA.
        3. **Zálohování serverů** – zálohování je čistě ze strany Operačního systému, pomocí nástroje třetí strany Veeam Agent for Microsoft Windows. Samotné zálohování probíhá denně na externí úložiště NAS Synology. Dostupnost zálohovaných dat je cca 14 dní zpětně.
        4. **Centrální management uživatelských účtů** – ve školní síti existuje jeden centrální management pro správu uživatelských účtů na platformě Microsoft Active Directory. Tyto účty jsou každých 30.min synchronizovány bezpečnou, šifrovanou formou do prostředí Microsoft Azure.

## Popis cílového stavu a specifikace předmětu plnění

### Základní požadavky na technické řešení

* + - 1. Cílem projektu je zvýšení bezpečnosti a související modernizace IT infrastruktury, aby implementací projektu byly naplněny Standardy konektivity škol [[1]](#footnote-1) (dále jen Standard konektivity, nebo Standard) a rozšířena funkčnosti ICT prostředí ZŠ a ZUŠ Petřvald, příspěvková organizace, podle Výzvy č. 10/2023 Konektivita škol – Moravskoslezský kraj. Dílčí cíle dle jednotlivých komodit jsou specifikovány následovně:

| Označení | Komodita | Počet |
| --- | --- | --- |
| K1 | Virtualizační platforma | 1 |
| K2 | Zabezpečení LAN a Wifi | 1 |
| K3 | Centrální logování | 1 |
| K4 | Systém správy identit – IDM | 1 |

* + - 1. 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.
      2. 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.
      3. 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 předpokládanou hodnotu zakázky.
      4. Zadavatel z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů vyžaduje v maximální míře 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. Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky a dodavatel splnění těchto podmínek potvrdí samostatným čestným prohlášením:
         1. jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
         2. mají plnou záruku od výrobce,
         3. mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
         4. obsahují všechny nezbytné licence na používání příslušného softwaru,
         5. jsou v databázi výrobce uvedeny jako prodaná kupujícímu,
         6. jsou určeny pro provoz v České republice.

Tyto skutečnosti dodavatel doloží čestným prohlášením distributora, popř. čestným prohlášením dodavatele, 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.

* + - 1. Veškerá dokumentace vytvořená v rámci realizace 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.

### Specifické požadavky na technické řešení

* + - 1. **K1 – Virtualizační platforma**
         1. 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 bude připojen do sítě duální optickou linkou 2x 10 Gb. Pořízený server musí být výrobcem určen pro provoz v běžném, neklimatizovaném prostředí do teploty 40 stupňů Celsia (krátkodobě až 45 stupňů Celsia) – např. dle ASHRAE Class A4.
         2. 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. Zálohovací systém umožní zálohovat i fyzické servery a osobní počítače. Sítové úložiště NAS bude kvůli bezpečnému oddělení záloh od produkčních dat umístěno mimo místnost serveru – optimálně v zabezpečené, uzamykané místnosti v jiné budově, části budovy.
         3. Provozní zabezpečení bude tvořeno souborem non-IT technologií, které zajistí optimální podmínky pro spolehlivý chod technologií – především serveru:

Záložní zdroj napájení UPS zajistí chod serveru při výpadku napájení

* + - * 1. 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 – systém IDM. Adresářová služby v MS AD budou synchronizovány ze systému IDM a 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, agenta 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 min. na 2 řadičích adresářové služby kvůli vysoké dostupnosti. Řadiče budou provozovány ve virtuálním prostředí a budou pravidelně automaticky zálohovány. Součástí řadičů budou základní síťové služby – DNS, DHCP, obě v konfiguraci pro vysokou dostupnost. 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.
      1. **K2 – Zabezpečení LAN a Wifi**
         1. Bude implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby s využitím technologie 802.1X.
         2. 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.
         3. Řízení provozu v LAN bude realizováno vytvořením VLAN (802.1Q), segmentací sítě s routováním (přepínáním) provozu mezi VLAN na úrovni firewallu s nastavitelnými ACL. Pro řízení provozu na úrovni kvality služeb bude k dispozici technologie QoS (Quality of Services). Pro zajištění vysoké výkonosti budou klíčové aktivní prvky propojeny opticky na rychlosti 1Gbit a vyšší.
         4. Architektura WiFi bude založena na řešení s centrální správou prováděnou virtuálním kontrolerem (řadičem), který bude součástí firmwarů přístupových bodů a 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.
         5. Umístění pořízených AP bude provedeno na základě provedené analýzy pokrytí signálem pro zajištění konzistentní WiFi služby v pokrytých prostorách. Provedení analýzy bude součástí projektu.
         6. Ověřování přístupu do LAN bude realizováno protokolem 802.1X, vůči adresářové službě prostřednictvím protokolů radius a P/EAP. V budoucnu pořizovaná zařízení (min. stolní i přenosné počítače) by měla být 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.
         7. Ověřování přístupu do WiFi sítě bude realizováno ověřováním jména a hesla na radius serveru vůči Active directory. Wifi bude nabízet více SSID (učitelé, žáci, Guest), které budou obsluhovány samostatnými VLAN a budou napojeny na radius servery. Učitelé a žáci budou prostřednictvím radius serveru ověřováni v adresářové službě. 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 před-generovaných číselných kupónů. Preferován bude captive portál firewallu s tzv. lobby přístupem pro správu a generování účtů/kupónů ne-technickou osobou.
      2. **K3 – Centrální logování**
         1. Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací – může jednat o jediné zařízení, softwarový nástroj či appliance. 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).
         2. 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.
         3. 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.
         4. 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.
      3. **K4 – Systém správy identit – IDM**
         1. IDM (dále IDM nebo Systém) bude udržovat a spravovat identity a organizační strukturu organizace – žáky, třídy, učitelský sbor, administrativa atd. Spravované identity budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy. Identity budou ukládány v databázi.
         2. Poskytnutá licence umožní nasazení a provoz IDM bez omezení na počet uživatelů, spravovaných identit a napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Zadavatele (počet záznamů, velikost databází atd.).

### Implementační služby

* + - 1. V rámci implementace předmětu plnění dodavatel realizuje pro všechny nabízené komodity K1 až K4 – následující služby:
         1. 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.
         2. Dodávka a implementace předmětu plnění dle schválené prováděcí dokumentace včetně technické podpory.
         3. Zajištění projektového vedení realizace předmětu plnění.
         4. 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 – zařazení počítače do domény, nastavení oprávnění

Zálohování – kontrola činnosti, obnova souborů

Hypervizor – ovládání virtuálních serverů, změna jejich konfigurace

Monitorovací a logovacího systém – vyhledávání činnosti uživatelů a systémů, běžná správa a kontrola funkce

LAN a Wifi – připojení zařízení vč. uživatelských postupů pro Wifi připojení mobilních zařízení (tablety, chytré telefony, notebooky) s operačními systémy Windows 10/11, Android, iOS a macOS.

Firewall – blokování stránek, dohledání činnosti uživatele, práce s kategoriemi stránek, zablokování přístupu pro uživatele skupinu

IDM – základní uživatelské činnosti se systémem IDM

* + - * 1. Zpracování dokumentu Zásady využívání ICT a přístupu k síti dle Standardu konektivity pro začlenění do vnitřních předpisů školy.
        2. Zpracování materiálů pro školení a provedení školení v rozsahu dle kapitoly 2.4
        3. Zajištění zkušebního provozu infrastruktury v délce minimálně 1 týdne včetně technické podpory specialistů na dané zařízení/službu s dostupností maximálně do 4 hodin na místě realizace od nahlášení požadavku v pracovní den v době od 8h do 17h.
        4. Provedení akceptačních testů.
        5. Předání do plného provozu.
      1. Činnost omezující práci uživatelů musí být prováděny primárně mimo běžnou pracovní dobu ZŠ, tj. mimo pracovní dny 7 – 15 hod. Ve výjimečných případech, a po vzájemné dohodě Zadavatele a Dodavatele, lze tyto práce provést i v pracovní době.
      2. 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.

|  |
| --- |
| K1: Virtualizační platforma |
| * 1. Návrh a kompletní implementace serverové virtualizační platformy   2. Implementace pořízených technologií   3. Analýza dat a systémů na stávajících serverech a jejich migrace na novou platformu   4. Návrh vhodné struktury Active Directory s redundantními řadiči, její vybudování a migrace stávající   5. Návrh a realizace zálohovacího řešení   6. konfigurace automatické odstávky a najetí serveru v případě výpadku a obnovení dodávky elektrické energie   7. Návrh a provedení akceptačních testů |
| K2: Zabezpečení LAN a Wifi |
| * 1. Analýza stávajícího síťového prostředí a návrh nového architektury LAN i WiFi   2. Implementace pořízených technologií   3. Provedení segmentace LAN – VLAN, adresování, routování   4. Zavedení IPv6 pro přístup k internetovým zdrojům publikovaným na IPv6 adresách (v součinnosti se Zadavatelem a jeho smluvními partnery)   5. Zavedení IPv6 pro veškeré publikované služby ZŠ z interních či externích prostředků. adresách (v součinnosti se Zadavatelem a jeho smluvními partnery)   6. Zabezpečení komunikace publikovaných služeb ZŠ pomocí nabízeného certifikátu. adresách (v součinnosti se Zadavatelem a jeho smluvními partnery)   7. Zavedení DNSSEC pro interní DNS služby.   8. Návrh a implementace 802.1X nebo PortSecurity 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   9. Návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) pro školu   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. Instalace ostatního HW, vybudování LAN rozvodů k AP   14. Zajištění ostatních nezbytných činností pro naplnění Standardu konektivity |
| K3: Centrální logování |
| * 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   1. Provedení souvisejících konfigurací monitorovaných systémů |
| K4: IDM |
| * 1. Návrh a implementace systému pro správu identit IDM   2. napojení na školský informační systém Bakaláři   3. napojení na MS AD a synchronizace identit do MS Azure AD pro MS Office 365 |

* + - 1. 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 https://opst.cz/dotace/10-vyzva/ , včetně úspěšného provedení a doložení testu. Prokázání naplnění požadavků poskytne dodavatel v písemné formě vhodné jako příloha k Závěrečné zprávě o realizaci projektu.
      2. Náklady na provedení implementačních služeb musí být zahrnuty v nabídkové ceně k položce (komoditě), ke které se vztahují a nelze je vyčíslit zvlášť.

### 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:
         1. běžných administrátorských činností pro implementované systémy
         2. 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 (celkem min. 10 hod), není-li uvedeno jinak. Školení bude probíhat v sídle zadavatele. Předpokládá se účast max. 3 osob.

### Harmonogram projektu

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

| Aktivita | Začátek | Termín |
| --- | --- | --- |
| Podpis smlouvy | D | D |
| Zahájení projektu – úvodní projektová schůzka | D | D+7 |
| Předimplementační analýza – zpracování | D+7 | D+14 |
| Předimplementační analýza – připomínkové řízení, schválení | D+14 | D+21 |
| Prováděcí dokumentace – zpracování | D+21 | D+30 |
| Prováděcí dokumentace – připomínkové řízení, schválení | D+30 | D+35 |
| Realizace předmětu plnění | D+35 | D+70 |
| Školení administrátorů | D+70 | D+80 |
| Zkušební provoz | D+80 | D+90 |
| Akceptační testy | D+80 | D+90 |
| Zahájení ostrého provozu | D+90 | - |
| Rezerva projektu |  | 10 |

* + - 1. Dodavatel může dle svého uvážení výše uvedené maximální lhůty trvání zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb.
      2. Maximální lhůty trvání nesmí dodavatel při tvorbě detailního harmonogramu prodloužit.
      3. Dodavatel uvede závazný harmonogram plnění ve své nabídce a zároveň v návrhu smlouvy.
      4. Dodavatel uvede potřebnou součinnost zadavatele pro splnění harmonogramu plnění ve své nabídce.

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

Popis povinných parametrů dodávaného řešení

* + - 1. 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.
      2. Dodavatel ve své nabídce detailně popíše způsob naplnění každého povinného parametru včetně značkové specifikace nabízených dodávek. Popis způsobu naplnění každého povinného parametru bude konkrétní, úplný a musí výslovně prokazovat, že nabízené řešení jednoznačně splňuje všechny aspekty povinného parametru.
      3. Dodavatel do tabulky povinných parametrů uvede odkaz na část nabídky, kde je možné ověřit naplnění parametru, tzn. na část nabídky s detailním popisem dle bodu (2). Vyplněné tabulky z tohoto oddílu technické specifikace učiní dodavatel součástí své nabídky.

**Celkový seznam dodávky:**

* Virtualizační server – 1ks
* SW licence serverových operačních systémů – 3ks
* SW přístupové licence k serveru, licence na zařízení – 210ks
* SW licence pro serverovou virtualizaci – 1ks
* UPS záložní zdroj – 1ks
* SW licence pro zálohování – 1ks
* Síťové úložiště NAS včetně HDD – 1ks
* NG Firewall – 1ks
* Páteřní přepínač – 1ks
* WiFi přístupové body (AP) – 49ks
* Přístupové přepínače – 24G PoE+ – 10ks
* Stohovatelní přístupové přepínače – 24G PoE+ – 4ks
* Stohovatelní přístupové přepínače – 48G PoE+ – 4ks
* Klimatizační jednotka do serverovny – 1ks
* Monitorovací a logovací systém – 1ks
* Identity management System – IDM – 1ks

1. Viz. <https://www.edu.cz/digitalizujeme/standard-konektivity-skol/> [10. výzva – Konektivita škol v Moravskoslezském kraji – Operační program Spravedlivá transformace (opst.cz)](https://opst.cz/dotace/10-vyzva/) [↑](#footnote-ref-1)