## Popis současného stavu

### Základní škola Habartov, Karla Čapka 119

* + - 1. Areál Základní školy Habartov, Karla Čapka 119 je umístěn na adrese Karla Čapka 119, Habartov a se skládá ze dvou pavilonů, tělocvičny a jídelny, viz. obrázek. V současné době navštěvuje školu 300 žáků a 55 zaměstnanců.

Obsah obrázku strom, dům, budova, Urbánní design

Popis byl vytvořen automaticky

* + - 1. Realizace projektu bude probíhat ve všech využívaných objektech.
      2. 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 Cat5e bylo budováno a rozšiřováno postupně podle aktuálních potřeb a finančních prostředků školy. Bezdrátové připojení je realizováno na úrovni standardu WiFi 5 a vyžaduje jen minimální rozšíření. Část použitých aktivních prvků sítě je již technicky i morálně zastaralých a výrobci nepodporovaných (nebo jen omezeně). Chybí významná provázanost a centralizovaná správa infrastruktury sítě.
      3. Kabelové rozvody byly provedeny kabely Cat5e. Pokrytí potřebných prostor budov metalickými rozvody je dostatečné. Bude potřeba doplnit jen minimum tras
      4. Aktuálně využívaný server výkonem a kapacitou vyhovuje aktuálním požadavkům, ale není schopen splnit všechny požadavky systému splňujícího požadavky Standardu konektivity.
      5. Server je aktuálně připojen rychlostí 1Gb/s do páteřního switche.
      6. 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. Některé aktivní prvky nesplňují požadavky na zabezpečení přístupu do LAN pomocí 802.1X.
      7. Internetové připojení je realizováno společností Wolfnet s.r.o. optickým kabelem s rychlostí 100 Mbps symetricky bez IPv6 konektivity. Rychlost připojení tak nedosahuje požadavek Standardu konektivity škol – 225 Mbps (300 žáků x 0,25 Mbps). Škola změní smlouvu se stávajícím poskytovatelem internetu, případně uzavře smlouvu s jiným poskytovatelem internetu tak, aby splnila minimální požadovanou rychlost připojení k internetu.
      8. Škola má přidělenu veřejnou IP adresu IPv4 Škola nemá v současné době validující DNSSEC resolver na straně školy, neprovádí pokročilý monitoring provozu.
      9. Škola provozuje Wifi síť, které pokrývá větší část školy a splňuje technologické požadavky kategorie WiFi 5. Tato WiFi síť slouží pro potřeby zaměstnanců i žáků školy. Síť má více SSID. Síť pro zaměstnance školy je chráněná silným heslem a má přístup k systémovým prostředkům školy. Síť pro žáky je chráněna heslem a uživatelé této sítě mají povolen pouze přístup do internetu. Síť je centrálně spravovaná.
      10. Zabezpečení přístupu k internetu využívá pouze NAT na hraničním prvku – routeru. Nejsou využívány pokročilé bezpečnostní funkce např. URL filtrace, antivirová kontrolou a detekce průniků.
      11. Škola provozuje jeden fyzický server s virtualizací. Jako hypervisor pro virtualizaci se používá řešení VMWare 6.5, je provozováno několik různorodých operačních systémů.
      12. 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.
      13. Škola disponuje centrální databází uživatelských identit Active Directory a využívá ji pro ověřování identity všech uživatelů přistupujících k síťových prostředků.
      14. Přístup do počítačů (resp. operačních systémů) je řízen převážně ověřováním vůči doméně Active Directory.
      15. 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.

## Popis cílového stavu a specifikace předmětu plnění

### Základní požadavky na technické řešení

* + - 1. V rámci projektu bude maximalizováno využití technických a systémových prostředků pořízených v předchozích projektech nebo vlastní investicí formou sdílení těchto prostředků 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 škol [[1]](#footnote-1) (dále jen Standard konektivity) a rozšířena funkčnosti ICT prostředí zapojených škol. Dílčí cíle dle jednotlivých komodit jsou specifikovány následovně:

|  |  |
| --- | --- |
| **Označení** | **Komodita** |
| A | Stavební úpravy, rozvody LAN |
| B | Zabezpečení LAN a Wifi |
| C | Centrální logování |
| D | Server, zálohování a licence operačních systémů |

* + - 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 zásadní uživatelské a provozní potíže.
      2. Je požadována unifikace jednotlivých komodit (tj. jejich realizace stejnými prostředky) pro všechny části z důvodu jednotné správy celého prostředí a odpovídající minimalizace provozních nákladů.
      3. 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.
      4. 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.
      5. 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.
      6. Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky a dodavatel splnění těchto podmínek potvrdí samostatným čestným prohlášením, které doloží do 15 dnů po podpisu smlouvy:
         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. 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.

* + - 1. 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.

### Specifické požadavky na technické řešení komodit

* + - 1. **A – Stavební úpravy, rozvody LAN** 
         1. Stavební úpravy zahrnují: úpravy podlah, elektroinstalace, slaboproudých rozvodů, prostupy, atd. dle specifikace v kapitole 01 ve výkazu výměr.
         2. Prostupy mezi požárními úseky budou provedeny v souladu s platným PBŘ.
         3. 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 komunikaci v rámci distribučních přepínačů.
         4. Všechny kabelové trasy (optické i metalické) bude proměřeny a měření budou doložena protokoly.
         5. Popis současného a budoucího stavu

Škola v současnosti nenaplňuje požadavky dle doporučení Standardů konektivity MŠMT. Stávající rozvody LAN jsou nedostatečné, logování provozu na síti žádné, školní síť není chráněna firewallem a nepodporuje IPV6.

**Rozdělení budov**

* Budova 1. stupeň
* Budova 2. stupeň
* Budova družina, jídelna, učebny

**Budova 1. Stupeň**

V této budově je centrální datový rozvaděč učebně VT v I.NP. Tento rozvaděč je nedostatečný a bude vyměněn za nástěnný rozvaděč 15U „Rack 1. stupeň-I.NP“. Z tohoto rozvaděče budou realizovány rozvody LAN a WiFi v I. NP v budově 1. stupně.

Podružný datový rozvaděč je nainstalován ve kabinetu č.32 ve II.NP. Tento rozvaděč je nedostatečný a bude vyměněn za nástěnný rozvaděč 15U „Rack 1. stupeň-II.NP“. Z tohoto rozvaděče budou realizovány rozvody LAN a WiFi v II. NP v budově 1. stupně.

Pasivní kabelové rozvody pro LAN jsou v pořádku a vyhovují požadavkům Standardů konektivity MŠMT. Nevyhovují pouze některé aktivní prvky, které budou nahrazeny novými. WiFi rozvody budou doplněny o jeden vysílač na každé patro.

Veškerá nově instalovaná kabeláž bude proměřena a měření doloženo protokolem.

* Rack 15 U 2 ks
* Switch 24 port PoE 2 ks
* Patch panel 24 port s cat. 6 Keystone konektorem 3 ks
* Vyvazovací panel 3 ks
* Napájecí panel 2 ks
* Optická vana s příslušenstvím 2 ks
* DAC kabel 3 ks
* WiFi AP 2 ks
* Optický modul FSP+ SM 3 ks
* Jednozásuvka na omítku s cat. 6 Keystone konektorem 2 ks
* Přívod napájení k rozvaděčům 2 ks

**Budova 2. stupeň**

Hlavní datový rozvaděč je nainstalován v kabinetu chemie ve III. NP. Tento rozvaděč je nedostatečný a bude nahrazen stojanovým rozvaděčem 42U „Rack 2. stupeň-III.NP“. Z tohoto rozvaděče budou realizovány rozvody LAN a WiFi ve III. NP v budově 2. stupně.

Podružný datový rozvaděč je nainstalován v kabinetu ve II.NP. Tento rozvaděč je nedostatečný a bude vyměněn za nástěnný rozvaděč 15U „Rack 2. stupeň-II.NP“. Z tohoto rozvaděče budou realizovány rozvody LAN a WiFi v II. NP v budově 2. stupně.

Další podružný datový rozvaděč je nainstalován v kabinetu dílen v I.NP. Tento rozvaděč je nedostatečný a bude vyměněn za nástěnný rozvaděč 15U „Rack 2. stupeň-I.NP“. Z tohoto rozvaděče budou realizovány rozvody LAN a WiFi v I. NP v budově 2. stupně.

Pasivní kabelové rozvody pro LAN jsou v pořádku a vyhovují požadavkům Standardů konektivity MŠMT. Nevyhovují pouze některé aktivní prvky, které budou nahrazeny novými. WiFi rozvody budou doplněny o jeden vysílač na každé patro.

Veškerá nově instalovaná kabeláž bude proměřena a měření doloženo protokolem.

* Rack 42 U 1 ks
* Rack 15 U 2 ks
* Switch 16 port PoE+ 1 ks
* Switch 24 port PoE 2 ks
* Switch 24 port 5 ks
* Patch panel 24 port s cat. 6 Keystone konektorem 5 ks
* Vyvazovací panel 5 ks
* Napájecí panel 3 ks
* Optická vana s příslušenstvím 3 ks
* DAC kabel 7 ks
* WiFi AP 3 ks
* Optický modul FSP+ SM 8 ks
* Jednozásuvka na omítku s cat. 6 Keystone konektorem 3 ks
* Přívod napájení k rozvaděčům 3 ks

**Budova družina, jídelna, učebny**

V této budově je datový rozvaděč nainstalován v oddělení ŠD. Tento rozvaděč je nedostatečný a bude demontován. Nový nástěnný rozvaděč „Rack družina“ bude nainstalován místo původního rozvaděče. Z tohoto rozvaděče budou realizovány veškeré rozvody LAN a WiFi v budově družiny, jídelny a učeben.

Pasivní kabelové rozvody pro LAN jsou v pořádku a vyhovují požadavkům Standardů konektivity MŠMT. Nevyhovují pouze některé aktivní prvky, které budou nahrazeny novými. WiFi rozvody budou doplněny o jeden vysílač na každé patro.

Veškerá nově instalovaná kabeláž bude proměřena a měření doloženo protokolem.

* Rack 15 U 1 ks
* Switch 24 port PoE 1 ks
* Patch panel 24 port s cat. 6 Keystone konektorem
* Napájecí panel 1 ks
* Optická vana s příslušenstvím 1 ks
* DAC kabel 1 ks
* WiFi AP 2 ks
* Optický modul FSP+ SM 1 ks
* Jednozásuvka na omítku s cat. 6 Keystone konektorem 2 ks
* Přívod napájení k rozvaděčům 1 ks

**Propojení datových rozvaděčů**

Rozvaděče budou mezi sebou propojeny optickým kabelem 4 vlákna single mode, které budou ukončeny v optických vanách konektorem SC.

* + - 1. **B** – **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 centrálního přepínače s nastavitelnými ACL. Pro řízení provozu na úrovni kvality služeb bude k dispozici technologie QoS (Quality of Services).
         4. Architektura WiFi 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.
         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. 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.
         7. Ověřování přístupu do WiFi sítě bude realizováno na stejném principu jako LAN (tj. protokol 802.1x + radius). Wifi 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 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.
         8. 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 WiFi 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.
      2. **C** – **Centrální logování**
         1. 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).
         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. 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.
         5. Technicky se může jednat o virtuální appliance nebo o samostatné komplexní řešení.
      3. **D** – **Server, zálohování a licence operačních systémů**
         1. 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.
         2. 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.
         3. Ochranou nově pořízených technologií vůči výpadku elektrického proudu bude UPS, která bude také pořízena v rámci projektu.
         4. Dodávka licencí pro hypervizor není součástí projektu – bude použita licence VMWARE 8, která je ve vlastnictví školy a má zajištěnou podporu do 2027/01.
         5. 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.
         6. Požadované licence operačních systémů musí umožnit využití implementovaných funkcionalit serverových řešení.
         7. 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.
         8. 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).

### Implementační služby

* + - 1. V rámci implementace předmětu plnění dodavatel realizuje pro všechny nabízené komodity následující služby:
         1. Provedení předimplementační analýzy (včetně plánovaných změn v konfiguraci současné infrastruktury) a zpracování detailního finálního popisu cílového stavu a postupu implementace.
         2. 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.
         3. Dodávka a implementace předmětu plnění dle schválené prováděcí dokumentace včetně technické podpory.
         4. Zajištění projektového vedení realizace předmětu plnění.
         5. 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 Wifi-připojení zařízení vč. podrobných uživatelských postupů pro Wifi připojení mobilních zařízení (tablety, chytré telefony, notebooky) s operačními systémy Windows 10 a vyšších, Android, iOS   
a MacOS.

* + - * 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 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.
        4. Provedení akceptačních testů.
        5. Předání do plného provozu.
      1. 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 výrobci a dle tzv. nejlepších praktik, i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné.

|  |
| --- |
| 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, 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 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 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 WiFi |
| 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   2. Návrh a provedení akceptačních testů, musí zahrnovat ověření logování veškerých požadovaných uživatelů a správnost přiřazení identit uživatelů logovaným údajům |
| **Server, 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. |
| Rozvody LAN |
| * 1. provedení detailního měření realizovaných metalických i optických rozvodů včetně přenosových parametrů (útlum, odrazy apod.), zhotovení a poskytnutí dokumentace měření. |

* + - 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 [Prokázání a kontrola naplnění standardu konektivity ve výzvách IROP (infrastruktura základních a středních škol)](https://irop.mmr.cz/getmedia/36c80ac4-db39-48f4-a730-4a4bea8f65aa/Standard-konektivity_overeni-a-kontrola_cerven-2017_final.pdf) 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.
      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, není-li uvedeno jinak. Školení bude probíhat v sídle zadavatele. Předpokládá se účast max. 3 osob.

## 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. 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.
      3. 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**.
      4. Vyplněné tabulky Komodit 1 až 5 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.
      5. **Ověření funkčních vlastností.** Zadavatel má právo vyzvat uchazeče k poskytnutí funkčních vzorků pro účely testování a ověření požadovaných funkčních vlastností, uchazeč je povinen doručit testovací vzorky zadavateli do deseti (10) pracovních dnů od doručení výzvy, a to na adresu uvedenou v této výzvě. Vybraný uchazeč poskytne testovací vzorky bezplatně a na dobu minimálně následujících patnáct (15) pracovních dnů, rovněž po tuto dobu poskytne součinnost s testováním. Testovací vzorky budou dodány v identické konfiguraci s nabízeným systémem a zadavatel ve výzvě jasně stanoví, jaké vzorky za účelem hodnocení nabídek požaduje. Ověření funkčních vlastností nabízeného systému bude provádět zadavatel, vycházeje z dokumentace k nabízenému systému. V případě nejasností zadavatel vyzve k účasti zástupce dodavatele/uchazeče, který mu poskytne potřebnou součinnost, a to maximálně do 5ti pracovních dnů po doručení výzvy uchazeči. Testy budou provedeny v prostředí zadavatele. Po ukončení testování budou funkční vzorky uchazeči vráceny (uchazeč si vyzvedne vzorky na vlastní náklady v místě plnění). Ověřování bude zakončeno vyhotovením zápisu. V případě, že testovaný systém neprojde úspěšným ověřením funkčních vlastností, neuzavře zadavatel s takovým uchazečem smlouvu.
      6. Zadavatel vyžaduje, aby nabízená řešení měla požadované funkce již v době podání nabídky, nikoliv aby se jednalo o budoucí funkce plánovaných verzí software pro nabízené řešení.

|  |  |  |  |
| --- | --- | --- | --- |
| **Komodita A – Stavební část** | | | |
| **Část** | **Parametr** | **Popis povinného parametru** | **Účastník uvede nabízený parametr** |
| **Stavební úpravy, kabelové rozvody včetně příslušenství** | Popis | Stavební úpravy, kabelové rozvody včetně příslušenství a souvisejících služeb dle podrobného výkazu výměr |  |
| Záruka | Kabelové rozvody 10 let, rozvaděče 24 měsíců |  |

| **Komodita B - Zabezpečení LAN a Wifi** | | | |
| --- | --- | --- | --- |
| **Část** | **Parametr** | **Popis povinného parametru** | **Účastník uvede nabízený parametr** |
| **B001**  **Perimetrový firewall 1ks** | Provedení | Umístitelné do racku |  |
| HW parametry | Počet síťových rozhraní LAN RJ45 1 Gb – min 14x |  |
| Počet rozhraní USB pro připojení ext. modemu - min. 1x |  |
| Výkon | Propustnost firewallu min. 20 Gb/s nezávisle na velikosti paketu |  |
| Propustnost firewallu - min. 15 Mpps (pps - paketů za sekundu) |  |
| Počet FW politik min. 10 000 |  |
| Počet současných otevřených spojení – min 1,5 M |  |
| Propustnost VPN - min. 11,5 Gbps |  |
| Propustnost IPS – min 2,6 Gbps |  |
| Propustnost antiviru - min. 1 Gbps |  |
| Funkce | Režim vysoké dostupnosti – Active Active, Active Passive, Clustering |  |
| 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 |  |
| Firewall | Možnost nastavovat firewall politiku na základě geografických údajů. |  |
| 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 |  |
| Filtrační funkce | Možnost výběru mezi file based režimem (buffer) nebo flow based (inspekce on-the-fly) |  |
| 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 2000 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 |  |
| Ověřování uživatelů | LDAP, Active Directory, Radius, TACACS+, Ověřování na základě certifikátu |  |
| 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. |  |
| Dynamické routování | RIP, BGP, OSPF, IS-IS |  |
| 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 |  |
| Reporty | Integrované logování a reporting, možnost vytváření vlastních reportů |  |
| SFP+ moduly a patch cordy | Součástí dodávky jsou potřebné originální SFP+ moduly a optické/metalické propojovací kabely pro realizace díla. |  |
| 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. |  |
| **B002**  **Přístupové přepínače 5 ks** | 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 výrobce zařízení, včetně nároku na nové verze firmware |  |
| **B003**  **Přístupové přepínače s PoE 5 ks** | 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 výrobce zařízení, včetně nároku na nové verze firmware |  |
| **B004**  **Kontrolér**  **1 ks** | Základní funkce | Kontrolér je určený pro řízení a správu switchů a WiFi 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 výrobce zařízení, a to včetně nároku na nové verze firmware |  |
| **B005**  **WiFi přístupové body vnitřní (AP) 7 ks** | Základní funkce | Přístupový bod (AP) standardu Wi-Fi 6 včetně montážního materiálu na stěnu nebo strop |  |
| Frekvence | podpora WiFi 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 WiFi 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-wifi rušení |  |
| Multi SSID | podpora vysílání min. 6 SSID (WiFi 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 výrobce zařízení, včetně nároku na nové verze firmware |  |
| **B006**  **Optické prvky** | Optický modul SFP+ 12 ks | Standards and Protocols IEEE 802.3ae, TCP/IP  Wave Length 1310 nm  Power Supply 3.3V  Fiber Type 9/125um Single-Mode  Max. Cable Length 10 km  Data Rate 10 Gbps  Port Type LC Duplex |  |
| **B007**  **Eduroam** | Popis | připojení do federovaného systému Eduroam |  |
| **B008**  **Systém 802.1X** | Popis | Instalace a konfigurace systému 802.1X pro zajištění autentizace uživatelů připojených přes LAN a WiFi prostředky do počítačové sítě školy. Systém je založený na protokolu RADIUS a je integrovaný s Active Directory |  |
| **B009 Centrální switch** | 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 výrobce zařízení, a to včetně nároku na nové verze firmware |  |

| **Komodita C - Centrální logování, monitoring síťového provozu** | | | |
| --- | --- | --- | --- |
| **Část** | **Parametr** | **Popis povinného parametru** | **Účastník uvede nabízený parametr** |
| **C001**  **Systém pro sběr a správu logů a monitoring síťového provozu 1x** | 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** | **Účastník uvede nabízený parametr** |
| **D001**  **Server 1x** | 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  2x 10 Gpps TP s využitím PCI slotu |  |
| 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 |  |
| **D002**  **UPS pro server 1 ks** | 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 |  |
| **D003**  **Zálohovací zařízení**  **1 ks** | 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 6TB HDD SATAIII/7200 RPM/256MB cache.  Disky se zárukou 36 měsíců, uvedené v seznamu kompatibilních disků výrobce zálohovacího zařízení. |  |
| 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 |  |
| **D004**  **UPS pro zálohovací zařízení**  **1 ks** | Provedení | Volně stojící |  |
| Příkon | Min. 950VA |  |
| Výkon | Min. 520W |  |
| Zásuvky | České zásuvky, minimálně 4 ks |  |
| Komunikace | USB port |  |
| Záruka | Min. 24 měsíců |  |
| **D005**  **SW licence zálohovací software**  **1ks** | Licence | Licence zálohovacího software pro min. 10 zálohovaných zařízení (nerozlišuje se mezi VM, fyzickýcm 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. |  |
| **D006**  **SW 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. |  |
| **D007**  **Klientské licence pro server** | Klientské licence | Klientské licence pro operační systém Windows Server v aktuální verzi umožňující využívat těchto systémů uživatelům celkem na 100 zařízeních. |  |

## Záruky a servisní podmínky

### Požadavky na záruky a servisní podmínky

* + - 1. Zadavatel uvádí u jednotlivých komodit, resp. jejich částí požadovanou min. záruku, popř. podporu. Uváděné parametry byly průzkumem trhu zjištěny jako standardní, tj. poskytovány výrobci jako součást standardní dodávky a ceny. Není-li záruka části uvedena, je pro tuto část požadována záruka min. 24 měsíců.
      2. Z důvodu zajištění udržitelnosti projektu požaduje zadavatel poskytnutí prodloužení záruky a záručního servisu vybraných komodit či jejich částí na 5 let. Cenu poskytnutí uvede dodavatel v Příloze č. 2 Kupní smlouvy – Cenová nabídka.
      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 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.

### Požadavky na zabezpečení provozu

* + - 1. Z důvodu zajištění udržitelnosti projektu po dobu 60 měsíců a zajištění bezpečnosti provozu požaduje zadavatel zajištění poskytnutí podpory softwarových produktů.
      2. Podpora je požadována minimálně v rozsahu potřebném pro zajištění bezpečného provozu dodaných systémů.
      3. V případě požadavku zadavatele je uchazeč povinen podporu v tomto rozsahu poskytnout. Cenu poskytnutí uvede dodavatel v Příloze č. 1 Kupní smlouvy – Kalkulace nabídkové ceny do určených polí v listu Provoz.

1. Viz. aktuální verze <https://www.edu.cz/digitalizujeme/standard-konektivity-skol/> [↑](#footnote-ref-1)