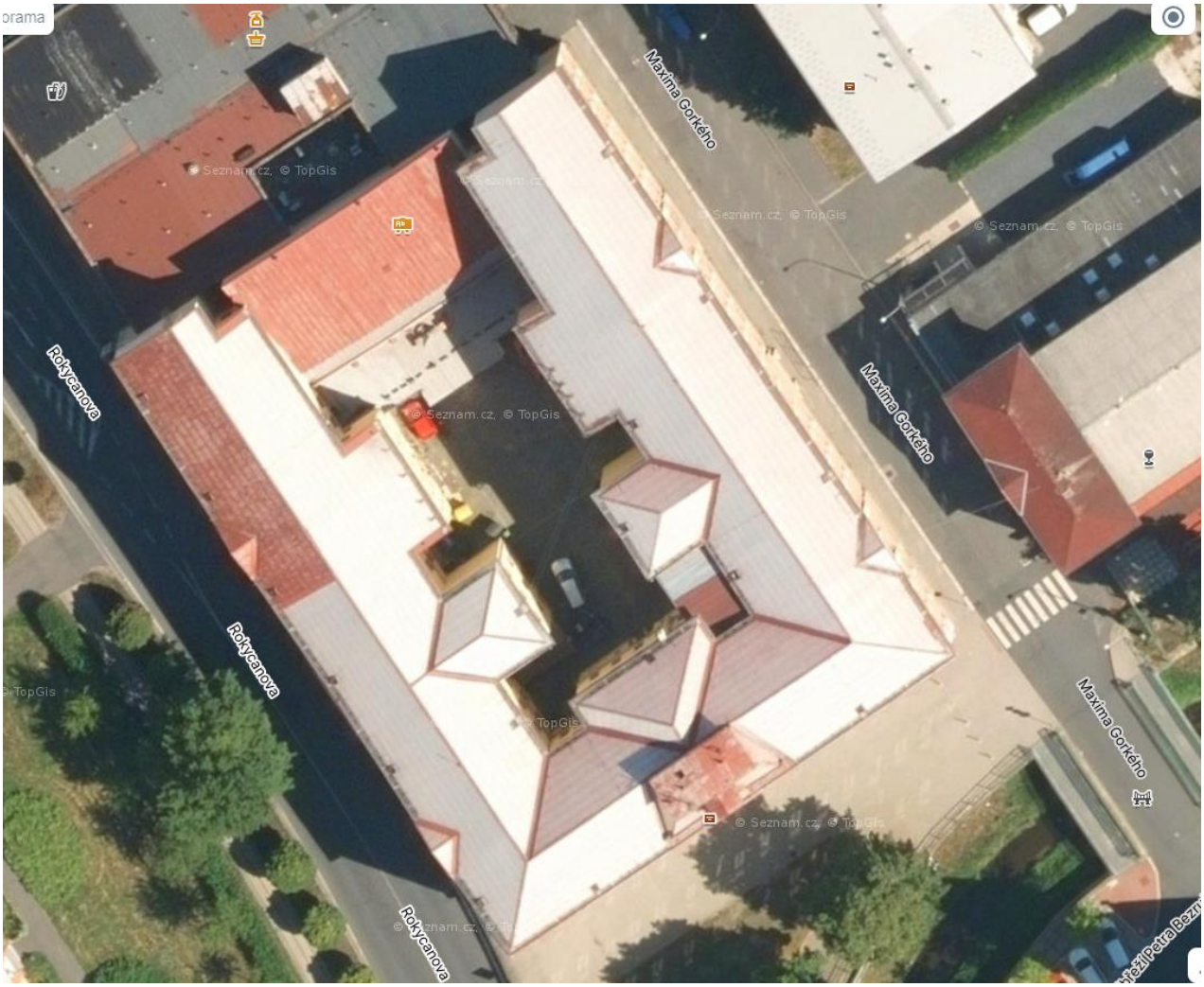
Příloha č. 5a - Současný stav a požadavky na technické řešení včetně projektové dokumentace

1. *Popis současného stavu a požadavky na technické řešení*

1.1. Základní škola Sokolov, Rokycanova 258

(1) Areál Základní školy Sokolov, Rokycanova 258 je umístěn na adrese Rokycanova 258 v Sokolově. V současné době navštěvuje školu přibližně 600 žáků a 55 učitelů a administrativních pracovníků.



(2) Realizace veřejné zakázky bude probíhat ve všech využívaných objektech.

(3) Současný stav ICT školy neodpovídá Standardu konektivity škol (dále jen Standard konektivity), a současným nárokům na výkon, bezpečnost a centralizovanou správu počítačové sítě. Počítačová síť byla budována postupně, staří a technická úroveň používaných prvků se výrazně liší. Síťové pokrytí na úrovni metalických kabelů Cat5 bylo budováno a rozšiřováno postupně podle aktuálních potřeb a finančních prostředků školy. Bezdrátové připojení bylo realizováno v minulosti na úrovni standardu WiFi 4 pro potřeby pokrytí aktuálních potřeb a s ohledem na omezené finanční možnosti, bez rezerv pro budoucí rozvoj. 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.

(4) Kabelové rozvody byly provedeny kabely Cat 5 a Cat5e. Pokrytí potřebných prostor budov metalickými rozvody je nedostatečné a neumožňuje připojovat do sítě další zařízení (koncová zařízení, IoT a bezpečností

prvky (kamery apod.) a síť rozvíjet např. doplňováním WiFi přístupových bodů. Nedostatek přípojných míst je na některých místech řešen „rozbočováním“ sítě malými přepínači bez managementu, jejichž použití dále komplikuje správu celé sítě a snižuje její robustnost, stabilitu a bezpečnost. Kabeláž je uložena převážně v lištách, občas „pod kobercem“.

(5) Aktuálně využívaný server výkonem a kapacitou nevyhovuje aktuálním požadavkům a není schopen splnit všechny požadavky Standardů konektivity.

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

(7) Propojení stanic i serverů je zajištěno přepínači 1 Gb/s bez možnosti pokročilé správy. Aktivní prvky nesplňují požadavky na zabezpečení přístupu do LAN pomocí 802.1X.

(8) Internetové připojení je realizováno společností Wolfstein s.r.o., optickou linkou s rychlostí 300Mbps symetricky bez IPv6 konektivity.

(9) Škola má nemá v současné době validující DNSSEC resolver na straně školy, neprovádí pokročilý monitoring provozu.

(10) Škola provozuje Wifi síť, které pokrývá pouze část školy a splňuje technologické požadavky kategorie WiFi 4. 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 není centrálně spravovaná. Použité prvky nepodporují aktuální bezpečnostní standardy (WPA3 apod.), ani pokročilé funkce optimalizace rádiového provozu a obsluhy připojených klientů.

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

(12) Škola nevyužívá žádný systém pro automatickou zálohu dat.

(13) Škola nedisponuje žádnou databází uživatelských identit a neověřuje tedy identitu uživatelů přistupujících k síťovým prostředkům.

Hlavní softwarovou platformou uživatelských počítačů jsou operační systémy společnosti Microsoft. Na koncových počítačích učitelů i žáků jsou používány převážně operační systémy Windows 10 a vyšší, s podporou domény Active Directory. Škola provozuje aktuálně téměř 150 zařízení. Správa životního cyklu operačních systémů a aplikačního vybavení se provádí manuálně.

1.2. Specifické požadavky na technické řešení komodit

V případě, pokud se liší počty jednotlivých položek uvedených v Příloze 5a – „Popis současného stavu a požadavky na technické řešení“ a počty položek uvedených v Příloze č. 4a – „Výkaz výměr“ pak platí, že závazné jsou počty položek uvedené v Příloze č. 4a – „Výkaz výměr“.

1.3. Komodita 01 – Rozvody LAN

I. NP

Rozvody LAN

Do každé učebny budou nataženy 4 kabely UTP cat 6. Do jídelny, tělocvičen a dílny budou nataženy 2 kabely UTP cat 6. Do kabinetů bude nataženo 6 kabelů UTP cat 6. Tyto kabely budou ukončeny dvojzásuvkou na omítku typu Keystone cat 6. V rozvaděčích v II. NP budou tyto kabely ukončeny v patch panelu Keystone cat 6.

Rozvody WiFi

Do každé učebny bude natažen kabel UTP cat 6. Na chodbu bude nataženo 6 kabelů UTP cat 6. Tyto kabely budou ukončeny jednozásuvkou na omítku typu Keystone cat 6. V rozvaděčích v II. NP budou tyto kabely ukončeny v samostatném patch panelu Keystone cat 6.

Veškerá kabeláž bude proměřena a měření doloženo protokolem.

- WiFi AP 18 ks
- Jednozásuvka na omítku s cat. 6 Keystone konektorem 18 ks
- Dvojzásuvka na omítku s cat. 6 Keystone konektorem 29 ks

II. NP

Stávající hlavní rozvaděč je nedostatečný a bude nahrazen rozvaděčem 42U, který bude umístěn do učebny VT. Zároveň bude doplněn podružnými nástěnnými rozvaděči 27U.

Rozvody LAN

Do každé učebny budou nataženy 4 kabely UTP cat 6. Do kabinetů bude nataženo 6 kabelů UTP cat 6. Do sborovny budou nataženy 2 kabely UTP cat 6. V učebně VT bude vytvořeno 32 přípojných míst. Tyto kabely budou ukončeny dvojzásuvkou na omítku typu Keystone cat 6. V rozvaděčích v II. NP budou tyto kabely ukončeny v patch panelu Keystone cat 6.

Rozvody WiFi

Do každé učebny, kanceláře školy, školního klubu, sborovny a ředitelny bude natažen kabel UTP cat 6. Na chodbu bude nataženo 5 kabelů UTP cat 6. Tyto kabely budou ukončeny jednozásuvkou na omítku typu Keystone cat 6. V rozvaděčích v II. NP budou tyto kabely ukončeny v samostatném patch panelu Keystone cat 6.

Veškerá kabeláž bude proměřena a měření doloženo protokolem.

- Rack 42 U 1 ks
- Rack 27 U 2 ks
- Switch 24 port 13 ks
- Switch 24 port PoE 3 ks
- Patch panel 24 port s cat. 6 Keystone konektorem 12 ks
- Vyvazovací panel 12 ks
- Napájecí panel 4 ks
- Optická vana s příslušenstvím 3ks
- Modul SFP+ SM 4 ks
- DAC kabel 13 ks
- WiFi AP 21 ks
- Jednozásuvka na omítku s cat. 6 Keystone konektorem 21 ks
- Dvojzásuvka na omítku s cat. 6 Keystone konektorem 42 ks
- Přívod napájení rozvaděče 3 ks

III. NP

Rozvody LAN

Do každé učebny budou nataženy 4 kabely UTP cat 6. Do kabinetů bude nataženo 6 kabelů UTP cat 6. V učebně chemie bude vytvořeno 32 přípojných míst. Tyto kabely budou ukončeny dvojzásuvkou na omítku typu Keystone cat 6. V rozvaděčích v II. NP budou tyto kabely ukončeny v patch panelu Keystone cat 6.

Rozvody WiFi

Do každé učebny, kabinetů V.3980, V.3950, V.3860 a V.4000 bude natažen kabel UTP cat 6. Na chodbu bude nataženo 5 kabelů UTP cat 6. Tyto kabely budou ukončeny jednozásuvkou na omítku typu Keystone cat 6. V rozvaděčích v II. NP budou tyto kabely ukončeny v samostatném patch panelu Keystone cat 6.

Veškerá kabeláž bude proměřena a měření doloženo protokolem.

- WiFi AP 21 ks
- Jednozásuvka na omítku s cat. 6 Keystone konektorem 21 ks
- Dvojzásuvka na omítku s cat. 6 Keystone konektorem 58 ks

1.4. Komodita 02 – Zabezpečení LAN a Wifi

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

(b) Pro hosty a externí uživatele bude zřízena samostatná VLAN (Guest VLAN), které bude komunikačně (min. L3 pravidla, ACL) oddělena od vnitřních sítí organizace. Tato VLAN bude mít své L3 rozhraní až na úrovní firewallu, tak aby bylo možné komunikaci podrobit kontrole za pomoci UTM nástrojů (min. AV, IPS, kategorizace obsahu) a mohl jí být přiřazen samostatný profil odlišný od profilů pro učitele a žáky. Ověřování přístupu do této VLAN bude zajištěno pomocí tzv. captive portálu – webové autorizace. Captive portál bude zajištěn firewallem případně jiným samostatným řešením nebo prvkem, ale vždy s důrazem na bezpečné oddělení uživatelského provozu od zbytku vnitřních sítí.

(c) Řízení 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).

(d) Architektura WiFi bude založena na řešení s centrální správou prováděnou hardwarovým nebo virtuálním kontrolérem (řadičem). Hardwarový nebo virtuální kontrolér 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.

(e) Součástí projektu bude i 1 ks venkovního přístupového bodu WiFi s technickými parametry uvedenými v příloze č. 7a – Popis povinných parametrů dodávaného řešení, položka B006 WiFi přístupové body venkovní (AP) 1 ks.

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

(g) 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.

(h) 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.

(i) 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.

1.5. Komodita 03 – Centrální logování, monitoring síťového provozu

(a) 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).

(b) 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.

(c) 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.

(d) 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.

(e) Technicky se může jednat o virtuální appliance nebo o samostatné komplexní řešení.

1.6. Komodita 04 – Server, diskové pole, UPS, zálohování a licence operačních systémů

(a) 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.

(b) 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.

(c) Ochranou nově pořízených technologií vůči výpadku elektrického proudu bude UPS, která bude také pořízena v rámci projektu.

(d) Dodávka licencí pro hypervizor není součástí projektu.

(e) 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.

(f) Požadované licence operačních systémů musí umožnit využití implementovaných funkcionalit serverových řešení.

(g) 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.

(h) Pro obvyklá zařízení využívaná 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).