

STŘEDNÍ ŠKOLA STRAVOVÁNÍ A SLUŽEB

KARLOVY VARY, příspěvková organizace



Veřejná zakázka s názvem
„SPRAVEDLIVÁ TRANSFORMACE – projekt Konektivita školy“
Autor: Pavel Lintemer

Technická dokumentace

1. Popis výchozího stavu

- (1) Areál Střední školy stravování a služeb Karlovy Vary, příspěvkové organizace tvoří budova s 6 nadzemními podlažími na adrese Ondřejská 1122/56, 360 01 Karlovy Vary - viz. obrázek. V současné době navštěvuje školu cca. 550 studentů.



- (2) Realizace projektu bude probíhat v celém objektu školy.
- (3) Současný stav ICT školy neodpovídá plně Standardu konektivity škol (dále jen Standard konektivity), a současným nárokům na výkon, bezpečnost a centralizovanou správu počítačové sítě. Počítačová síť byla budována postupně, staří a technické úroveň používaných prvků se liší. Síťové pokrytí – drátové i bezdrátové – bylo v jednotlivých etapách realizováno na pokrytí aktuálních potřeb a s ohledem na omezené finanční možnosti, bez rezerv pro budoucí rozvoj. Část prvků je technicky i morálně zastaralých a výrobci nepodporovaných, nebo jen omezeně. Chybí provázanost jednotlivých částí. Chybějící systém správy identit neumožňuje automatizované udržování individuálních elektronických identit pro všechny uživatele sítě (studenty i učitele) a následné automatické uplatňování politik pro řízení, monitorování a logování síťové a internetové komunikace. Absence možnosti detailního řízení a sledování provozu je klíčovou překážkou ve zvýšení úrovně kybernetické bezpečnosti a realizaci preventivních opatření. Decentralizovaná, resp. roztržitá správa sítě bez podpůrných a automatizačních nástrojů vyčerpává kapacitu správce sítě opakovanými rutinními činnostmi a nedává časový prostor pro systematický a koncepční rozvoj a podporu uživatelů.
- (4) Metalické kabelové rozvody v budově jsou provedeny kabely Cat 6, optické spoje mezi datovými rozvaděči v 2. a 6. NP jsou provedeny single modovými vlákny. Kabeláže je vybudována jako strukturovaná, ale pokrytí budovy metalickými rozvody je nedostatečné a neumožňuje připojovat do sítě další zařízení, především WiFi přístupové body a bezpečností a IoT prvky (kamery apod.) a síť tak rozvíjet. Nedostatek přípojných míst je řešen „rozbočováním“ sítě malými přepínači bez managementu, jejichž použití dále komplikuje správu celé sítě a snižuje její robustnost, stabilitu a bezpečnost. Kabeláž je uložena převážně ve vkladacích lištách a kabelových kanálech. Datové rozvaděče jsou uzamykatelné.
- (5) Propojení stanic i serverů je zajištěno převážně přepínači 100 Mb/s, částečně 1 Gb/s bez možnosti (pokročilé) správy. Aktivní prvky jsou umístěny převážně v datových rozvaděčích a jsou dostatečně zabezpečeny proti neoprávněné manipulaci. Škola nevyužívá segmentaci VLAN, síť tvoří jednu kolizní doménu, a to se negativně projevuje na její propustnosti a spolehlivosti. Aktivní prvky nesplňují požadavky na zabezpečení přístupu do LAN pomocí 802.1X.

- (6) Internetové připojení v současnosti zajišťuje společnost WolfNet prostřednictvím spoje o rychlosti 300/300 Mbps. Rychlost připojení tak s rezervou odpovídá požadavku Standardu konektivity ¹ – 137,5 Mbps (550 studentů x 0,25 Mbps).
- (7) Škola nemá přiděleny veřejné IP adresy IPv4 ani IPv6. Škola nemá v současné době validující DNSSEC resolver na straně školy, neprovádí pokročilý monitoring provozu. Škola provozuje 1 doménu - ssstravovani.cz.
- (8) Škola provozuje spojení WiFi s částečným pokrytím. Slouží pouze pro potřeby zaměstnanců školy. Přístup k síti je zabezpečený sdíleným heslem. Síť je omezeně centrálně spravovaná a použité prvky nedisponují podporou dostatečného počtu VLAN a jejich automatického přidělování pro segmentaci sítě školy. Prvky nepodporují aktuální bezpečnostní standardy (WPA3 apod.) ani pokročilé funkce optimalizace rádiového provozu a obsluhy připojených klientů.
- (9) Zabezpečení přístupu k internetu využívá pouze základní NAT na hraničním routeru bez jakýchkoli pokročilých bezpečnostních funkcí – např. URL filtrace, antivirové kontroly a detekce průniků. Nelze provádět inspekci ssl/https provozu, který je převažující a nejsou k dispozici moderní bezpečnostní funkce – např. sandboxing.
- (10) Škola provozuje dva fyzické servery, jeden je virtualizován pomocí Microsoft Hyper-V. Operační systém serverů je Windows 2012R2 a je využíván pro sdílení souborů, zajištění základních síťových služeb (DNS, DHCP) a adresářových služeb Active Directory.
- (11) Zálohování serverů provádí základní nástroj integrovaný v operačním systému, zálohy jsou ukládány externí USB disk. Kapacita systému není dostatečná pro zálohování dalších systémů (např. virtuálních serverů) a realizaci pokročilé ochrany záloh před kompromitací např. snapshoty či obdobnou technologií.
- (12) Škola disponuje dvěma oddělenými centrálními databázemi uživatelských identit Active Directory – samostatně pro studenty a učitele, ale neprovozuje žádný systém pro automatizovanou a jednotnou správu identit a řízení jejich oprávnění – IDM (Identity Management).
- (13) Přístup do počítačů (resp. operačních systémů) je řízen sdílenými uživatelskými účty (studenti) a osobními uživatelskými účty (učitelé), které jsou ověřovány vůči Active Directory.
- (14) Hlavní softwarovou platformou serverů i uživatelských počítačů jsou operační systémy společnosti Microsoft. Na koncových počítačích učitelů i studentů jsou používány převážně operační systémy Windows 10 a vyšší s podporou domény Active Directory. Škola provozuje cca. 160 počítačů. Správa životního cyklu operačních systémů a aplikačního vybavení se provádí manuálně. Ochrana počítačů před škodlivým software je zajišťována systémem Microsoft Defender v základní verzi obsažené v operačním systému a bez centrální správy a dohledu.
- (15) Pro zajištění potřebných licencí produktů Microsoft škola využívá multilicenční smlouvu, který mj. jiné zahrnuje i aktuální klientské licence Windows Server.
- (16) Škola využívá cloudových služeb Microsoft 365.
- (17) Škola využívá a prostřednictvím internetu vzdáleně zpřístupňuje webové aplikace – internet školy (<https://www.ssstravovani.cz>), školský informační systém Škola OnLine (<https://www.skolaonline.cz/>) a stravovací systém (<https://strava.cz>). Aplikace jsou publikovány na IPv4 a částečně na i IPv6 adresách, jsou dostupné šifrovaným protokolem https zabezpečeným certifikáty vydanými veřejnými certifikačními autoritami.
- (18) Škola využívá kamerový systém s částečným (nedostatečným) pokrytím vnitřních a vnějších prostor. Stávající záznamová zařízení nemají kapacitu a výkon pro obsluhu dalších kamer.

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

2. Popis cílového stavu a specifikace předmětu plnění

2.1. Základní požadavky na technické řešení

- (1) Cílem projektu je zvýšení bezpečnosti a související modernizace IT infrastruktury, aby implementací projektu byl naplněn Standard konektivity a rozšířena funkčnosti ICT prostředí školy. Dílčí cíle jednotlivých komodit jsou specifikovány následovně:

Označení	Komodita	Počet
K1	Virtualizační platforma	1
K2	Zabezpečení LAN a WiFi	1
K3	Centrální logování a správa identit	1
K4	Koncová zařízení	1
K5	Kabelové rozvody LAN	1

- (2) Je požadováno řešení zachovávající a rozvíjející současné softwarové serverové i desktopové platformy Microsoft pro zachování kompatibility se stávajícími systémy a výukovými a provozními aplikacemi. Přejed na jinou platformu by způsobil uživatelské a provozní potíže.
- (3) Pokud dodavatel vyžaduje využití konkrétních softwarových produktů a jím zvolený přístup k realizaci zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.
- (4) 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.
- (5) 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) jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
 - (b) mají plnou záruku od výrobce,
 - (c) mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
 - (d) obsahují všechny nezbytné licence na používání příslušného softwaru,
 - (e) jsou v databázi výrobce uvedeny jako prodaná kupujícímu,
 - (f) jsou určeny pro provoz v České republice.

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

- (7) Veškerá dokumentace 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. Struktura i forma dokumentace musí být před předáním předána ke kontrole a výslovně schválena zadavatelem.

2.2. Specifické požadavky na technické řešení

(1) K1 – Virtualizační platforma

- (a) Serverové technologie a hlavní síťové prvky budou umístěny ve stávajícím datovém rozvaděči v neklimatizované místnosti.
- (b) 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 10 Gb síťovou linkou. Pořízený server musí být výrobcem určen pro provoz v běžném, neklimatizovaném prostředí do teploty min. 35 stupňů Celsia.
- (c) Pro zálohování bude v rámci projektu pořízeno síťové úložiště NAS s dostatečnou kapacitou pro ukládání provozních záloh všech virtuálních serverů a archivů logů monitorovacího a logovacího systému.

Zálohování bude řízeno pokročilým zálohovacím software, který bude prostřednictvím virtualizačního hypervizoru zálohovat všechny virtuální servery. Zálohovací systém zajistí ochranu záloh před poškozením a umožní zálohovat i důležité osobní počítače.

- (d) Provozní zabezpečení bude tvořeno souborem non-IT technologií, které zajistí optimální podmínky pro spolehlivý chod technologií – především serveru:
 - (i) Záložní zdroje napájení UPS zajistí chod serveru a síťových přepínačů při výpadku napájení
 - (ii) Uzamykatelný rack zajistí bezpečné uložení serveru, správné větrání a zamezí neoprávněné manipulaci se serverem
- (e) Pro zajištění bezpečnosti a možnosti řízení provozu v síti a zajištění prokazatelného monitoringu, logování a auditu interního i externího síťového provozu bude aktualizována a zkonsolidována centrální databáze identit na bázi adresářové služby Active Directory. Adresářová služba umožní ukládání a přehlednou správu identit (účetů 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, agenty firewallů a dalších. Adresářová služba zajistí ověřování uživatelů pro účely jejich autorizace k přístupu k síťovým prostředkům (LAN, internet atd.) i výpočetním zdrojům (pracovní stanice, tiskárny, sdílené složky atd.). Technické provedení bude založeno na softwarovém řadiči adresářové služby. Řadič bude provozován ve virtuálním prostředí a bude pravidelně automaticky zálohován. Součástí řadiče budou základní síťové služby – DNS, DHCP. Ověřování identit musí být dostupné i systémům, které přímo nepodporují LDAP nebo jiný protokol adresářové služby. Součástí projektu bude proto i vybudování tzv. zprostředkovatelů identit, které umožní ověřování i jinými protokoly. Technicky půjde o softwarové komponenty transformující požadavky na ověření identity do formátu akceptovaného adresářovou službou.
- (f) Součástí platformy budou 1 terminálový server pro bezpečný chod provozních agend s možností bezpečného vzdáleného přístupu i prostřednictvím veřejných sítí (např. internetu) s využitím hardwarových nebo softwarových tenkých klientů.

(2) K2 – Zabezpečení LAN a WiFi

- (a) V rámci komodity budou do stávajících datových rozvaděčů dodány a osazeny nové aktivní prvky (firewall a přepínače), které budou doplněny zdroji záložního napájení (UPS). Pro bezdrátovou komunikaci WiFi budou nasazeny moderní přístupové body (AP – access point) standardu WiFi 6.
- (b) Bude implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby s využitím technologie 802.1X.
- (c) Pro hosty a externí uživatele bude zřízena samostatná VLAN (Guest VLAN), které bude komunikačně (min. L2 VLAN, L3 pravidla, ACL) oddělena od vnitřních sítí organizace. Tato VLAN bude mít své L3 rozhraní až na úrovni 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.
- (d) Řízení provozu v LAN bude realizováno vytvořením VLAN (802.1Q), segmentací sítě s routováním (směrováním) provozu mezi VLAN na úrovni centrálního přepínače s nastavitelnými ACL. Pro řízení provozu na úrovni kvality služeb bude k dispozici technologie QoS (Quality of Services). Pro zajištění vysoké dostupnosti služeb budou klíčové aktivní prvky propojeny duálními trasami s automatickým rozkládáním zátěže a převzetím služeb v případě výpadku jedné trasy.
- (e) Architektura WiFi bude založena na řešení s centrální správou prováděnou kontrolerem (řadičem), který bude součástí firmwaru síťových prvků a zajistí automatické rozložení zátěže klientů, roaming mezi spravovanými přístupovými body a trvalou automatickou detekci a reakci na rušení cizím signálem.
- (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. Nabízená zařízení (min. stolní i přenosné počítače) musí vybavena tzv. suplikantem–softwarovou komponentou, která dokáže předávat ověřovací požadavky síťovým prvkům, které tyto požadavky ověří vůči adresářové službě. Pro ověření zařízení bez 802.1X suplikantů (např. starší tiskárny, zařízení na bázi jednoduchých operačních systémů či firmware apod.) bude použit jiný,

dodavatelem navržený a 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, eduroam), 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 WPA2/3 s AES šifrováním a konfigurováno shodně pro obě frekvenční pásma. Výjimkou bude síť určená výhradně pro hosty (Guest WiFi), kde bude realizován tzv. captive portál zajišťující webovou autentizaci hostů pomocí přidělených účtů nebo za pomoci předgenerovaných číselných kupónů. Preferován bude captive portál firewallu s tzv. lobby přístupem pro správu a generování účtů/kupónů netechnickou osobou.
- (i) Federovaný systém EDUROAM (<http://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 uživatelské identity (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 EDUROAM 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.
- (j) Pro zabezpečení veřejně publikovaných služeb a webových management nástrojů bude implementován certifikát veřejné certifikační autority, jejíž certifikát je standardně obsažen v seznamu důvěryhodných autorit v obvyklém operačních systémech (Windows, Linux, Android, IOS/macOS/iPadOS).

(3) K3 – Centrální logování a Správa identit

- (a) Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací – může se jednat o softwarový nástroj či appliance. Řešení umožní správu z jedné grafické konzole, přístupné nativně skrze https bez nutnosti instalace klienta. Data budou ukládána do jedné databáze (nebo více vzájemně 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. 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.
- (d) Kombinací požadavků Zákona o uchování informací v elektronické komunikaci spolu s požadavky Standardu konektivity škol a praktického pohledu na možné časové prodlžení 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 a optimalizován, především z hlediska hospodaření s diskovou kapacitou, RAM i CPU, tak aby nedocházelo k výkonovým ani kapacitním problémům a systém měl dostatečnou rezervu pro očekávatelný budoucí nárůst informací a jejich zdrojů.
- (e) V rámci komodity bude dále implementován systém pro správu identit (IDM – Identity management, nebo dále též systém). Systém bude čerpat údaje o uživateli (identitách) se školského informačního systému a bude umožňovat doplňovat uživatele ručně, pokud nejsou v systému zavedeni. Systém musí umožnit změnu zdroje identit (tj. školského informačního systému) konfigurací IDM bez potřeby programových úprav systému.

- (f) IDM bude na základě atributů uživatele (např. třída, doba studia apod.) a zadaných pravidel automaticky vytvářet/měnit/mazat uživatelské účty a nastavovat jejich oprávnění v řízených systémech. Automaticky tak bude vytvářeno a průběžně upravováno pracovní prostředí žáků a učitelů v počítačové síti (přihlášení do sítě, přístup k programům a datům, přístup k internetu, mapování sdílených složek a tiskáren atd.) tak, aby vždy odpovídalo nastaveným pravidlům a aktuálním atributům uživatele.
 - (g) Součástí systému pro správu identit bude detailní logování prováděných změn pro možnost zjištění uživatelských oprávnění v libovolném času v minulosti (od nasazení systému).
 - (h) Automatizací správy identit dojde k odstranění nebo alespoň významnému omezení rutinních činností správců systémů spojených se správou identit a dále ke zrychlení reakcí na změny v organizaci (např. nástup/výstup žáků), snížení chybovosti způsobené ručním zadáváním údajů do systémů a/nebo nedodržení procesů (např. včasným nenahlášením odchodu zaměstnance nedojde včas nebo vůbec ke zrušení přístupových účtů zaměstnance) a získání okamžitého detailního přehledu o stavu identit a jejich oprávnění v systémech škol.
 - (i) Implementace systému bude provedena v souladu s § 19 Správa a ověřování identit Vyhlášky č. 82/2018 Sb. Zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.
- (4) **K4 – Koncová zařízení**
- (a) Součástí komodity je dodávka koncových zařízení v návaznosti na centrální serverové systémy.
 - (b) Pro každé nabízené zařízení určené k připojení do počítačové sítě bude předvedena vzorová konfigurace (min. 1 vzorek), předvedena plně funkcionální zařízení v síti, provedeno seznámení s vazbami zabezpečení sítě na konfiguraci zařízení a demonstrováno logování provozu zařízení a činnost jeho uživatele.
- (5) **K5 – Kabelové rozvody LAN**
- (a) V rámci komodity bude rozšířen současný strukturovaný kabelový systém. Systém zajistí spolehlivou komunikaci centrálních (serverových) technologií, napojení na stávající rozvody a dále napojení dodaných přístupových bodů WiFi, včetně jejich napájení.
 - (b) Centrálně bude umístěn hlavní datový rozvaděč pro uložení serverových a bezpečnostních technologií.
 - (c) Metalické kabelové rozvody budou provedeny metalickými kabely CAT 6, optické rozvody single modovými vlákny.
 - (d) Metalická i optická kabeláž bude respektovat již vytvořené kabelové trasy z původního projektu z roku 2016 (Součást přílohy č. 2 zadávací dokumentace). Při realizaci tohoto projektu nebudou realizovány žádné nové trasy ani prostupy.

2.3. Implementační služby

- (1) V rámci implementace předmětu plnění dodavatel realizuje pro všechny nabízené komodity K1 až K6 – následující služby, **kteřé jsou zahrnuté v ceně dodávky**:
- (a) Zpracování detailního finálního popisu cílového stavu a postupu implementace (včetně plánovaných změn v konfiguraci současné infrastruktury) a provedení související nezbytné analýzy současného stavu. Výstupem bude prováděcí dokumentace, podle které bude dodavatel řešení implementovat. Prováděcí dokumentace musí být před zahájením implementace výslovně schválena zadavatelem. Prováděcí dokumentace musí respektovat a využívat osvědčené praktiky (tzv. Best Practice) a doporučení výrobců nabízených technologií.
 - (b) Dodávka a implementace předmětu plnění dle schválené prováděcí dokumentace včetně technické podpory.
 - (c) Zajištění projektového vedení realizace předmětu plnění.
 - (d) Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení popisu činností běžné údržby a činností pro spolehlivé zajištění provozu. Popis činností běžné údržby bude pokrývat minimálně následující oblasti:
 - (i) Adresářová služba – správa uživatelů a skupin, zařazení počítače do domény
 - (ii) Zálohování – kontrola činnosti, obnova souborů
 - (iii) Hypervizor – ovládání virtuálních serverů, změna jejich konfigurace

- (iv) Logovací systém – vyhledávání činnosti uživatelů a systémů, běžná správa a kontrola funkce
- (v) LAN a WiFi – připojení zařízení vč. podrobných uživatelských postupů pro WiFi připojení mobilních zařízení (tablety, chytré telefony, notebooky) s operačními systémy Windows 10 a vyšší, Android, iOS, macOS a iPadOS.
- (vi) Firewall – blokování stránek, dohledání činnosti uživatele, práce s kategoriemi stránek, zablokování přístupu pro uživatele skupinu
- (vii) Systém pro správu identit – podrobná příručka pro správce i uživatele v českém jazyce
- (e) Zpracování dokumentu Zásady využívání ICT a přístupu k síti pro začlenění do vnitřních předpisů školy.
- (f) Zpracování materiálů pro školení a provedení školení v rozsahu dle kapitoly 2.4.
- (g) Zajištění zkušebního provozu infrastruktury v délce minimálně 2 týdnů včetně technické podpory specialistů na dané zařízení/službu s dostupností maximálně do 4 hodin od nahlášení požadavku v pracovní den v době od 8h do 17h.
- (h) Provedení akceptačních testů.
- (i) Předání do plného provozu.
- (2) Činnost omezující práci uživatelů musí být prováděny mimo běžnou pracovní dobu školy, tj. mimo pracovní dny 7-15 hod.
- (3) Zadavatel dále požaduje provést minimálně následující implementační práce na dodaných komponentech a případně dalších zařízeních. Dodavatel je dále povinen zahrnout do nabídky veškeré další činnosti a prostředky, které jsou nezbytné pro provedení díla v rozsahu doporučeném výrobcem a dle tzv. nejlepších praktik, i v případě, že nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné.

K1: Virtualizační platforma	
a)	Návrh a kompletní implementace serverové virtualizační platformy včetně systému terminálových služeb s publikační bránou do veřejných sítí
b)	Implementace pořízených technologií
c)	Analýza dat a stávajících sdílených systémů a jejich migrace na novou platformu
d)	Návrh vhodné struktury adresářové služby, její vytvoření a naplnění identitami
e)	Návrh a realizace zálohovacího řešení včetně nastavení zálohovacích plánů.
f)	Implementace automatické odstávky serveru v případě výpadku dodávky elektrické energie
g)	Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy a testy vysoké dostupnosti, je-li architektura tak navržena.
K2: Zabezpečení LAN a WiFi	
a)	Analýza stávajícího síťového prostředí a návrh nového architektury LAN i WiFi
b)	Implementace pořízených technologií
c)	Provedení segmentace LAN – VLAN, adresování, směrování
d)	Zavedení IPv6 pro přístup k internetovým zdrojům publikovaným na IPv6 adresách
e)	Zavedení IPv6 pro veškeré publikované služby školy z interních či externích prostředků. Včetně zajištění podpory jednání a řízení změn u externích poskytovatelů služeb. Jde zejména o služby hostování domény ssstravovani.cz , DNS, e-mail, web školy, popř. publikace školského systému pro rodiče
f)	Zabezpečení komunikace publikovaných služeb školy pomocí certifikátu.
g)	Zavedení DNSSEC pro interní DNS služby i zabezpečení domény ssstravovani.cz
h)	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, iPadOS, embedded systémy periferií
i)	Návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) pro školu
j)	Vybudování VPN pro vzdálený přístup uživatelů LAN na bázi webového portálu
k)	Respektování min. 3 různých skupin uživatelů (učitelé, studenti, hosté) v návrzích a implementaci bezpečnostních a ostatních politik
l)	Implementace portálu pro registraci a řízení přístupů hostů – tzv. captive portál
m)	Implementace připojení k EDUROAM a zpřístupnění v prostorech školy včetně zajištění jednání a řízení změn s provozovatelem (CESNET) a organizačních opatření – zpracování textů pro web školy, zapracování do Zásad využívání ICT
n)	Zajištění ostatních nezbytných činností pro naplnění Standardu konektivity

K3: Centrální logování a Správa identit	
<u>Centrální logování</u> a) 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 zařízení • automatizace kontrol monitorovaných systémů z pohledu chování, zranitelností, konfigurace apod. b) Provedení souvisejících konfigurací monitorovaných systémů <u>Správa identit</u> Předimplementační analýza bude obsahovat následující oblasti specifické pro komoditu: - provedení analýzy ICT prostředí školy se zaměřením na oblast správy uživatelských účtů, přidělování oprávnění a rolí, - technologický popis stávajících technologií s vazbou na systém správy identit - návrh životního cyklu identity uživatelů, - model organizační struktury, - přiřazení zaměstnanců a žáků k pracovním pozicím a rolím - atributy poskytované školským informačním systémem ve vazbě na řízené systémy a návrh jejich využití, - analýzu možností správy výstupních struktur, - analýzu evidenčních údajů a logů, - analýzu a návrh řízení identit a jejich oprávnění v řízených (napojených) systémech Další požadované služby - kompletní implementace systémů dle předimplementační analýzy a prováděcí dokumentace - metodické a odborné vedení pracovníků škol při jednání o poskytnutí potřebných rozhraní na straně školského informačních systémů. Případné náklady na rozhraní nejsou součástí této zakázky - návrh a provedení akceptačních testů, musí zahrnovat výkonové testy a prokázat plnou funkčnost integrací v obvyklých scénářích použití	
K4: Koncová zařízení	
- Dodávka a zprovoznění vzorových zařízení včetně potřebných montážních prací - U operačních systémů nabízených zařízení není požadováno provedení aktivace a konfigurace operačního systému a instalace kancelářského balíku – s výjimkou vzorku viz. 2.2(4)(b). Uvedené činnosti provede zadavatel vlastními silami dle připraveného vzorku a dodavatelem poskytnuté dokumentace.	
K5: Kabelové rozvody LAN	
Dodávka a kompletní oživení kabelového systému včetně certifikačního měření prokazujícího splnění standardů Cat6 a požadovaných parametrů systému poskytovaných po dobu záruky	

- (4) Akceptační testy musí pro všechny komodity vždy zahrnovat minimálně prokázání kompletnosti dodávky a požadované funkčnosti, dále prokázání aktivací software i hardware aktivačními klíči či jinými prostředky, je-li aktivace potřebná. Dále pro každou komoditu navrhne dodavatel vhodné doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost a odpovídající výkon a stabilita dodaného řešení. Návrh vhodných akceptačních kritérií bude součástí Prováděcí dokumentace.

- (5) Povinným akceptačním kritériem bude prokázání naplnění požadavků Standardu konektivity dle manuálu uveřejněného na <https://www.edu.cz/digitalizujeme/standard-konektivity-skol/#prokazani> včetně úspěšného provedení a doložení testu na <https://www.standardkonektivity.cz/>.

Prokázání naplnění požadavků poskytne dodavatel následně v písemné formě jako přílohu k Závěrečné zprávě o realizaci projektu. Standard konektivity školy SŠSS Karlovy Vary tvoří přílohu č. 8 zadávací dokumentace (je upřesněn v doporučených parametrech).

Zadavatel proto požaduje od dodavatele vyplnit čestné prohlášení, že jeho nabídka splňuje požadavky tohoto standardu konektivity, toto čestné prohlášení je součástí přílohy č. 6 Technická specifikace nabízeného řešení.

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

2.4. Školení

- (1) Dodavatel provede pro každou komoditu odborné školení na obsluhu a práci s dodanými zařízeními, a to minimálně v rozsahu provozní dokumentace.
- (2) Školení bude pokrývat všechna zařízení a systémy všech komodit, dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu:
- (a) běžných administrátorských činností pro implementované systémy
 - (b) standardní údržby systémů pro administrátory zadavatele
- (3) Školení dále zajistí seznámení pracovníků zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.
- (4) Minimální rozsah školení pro každou komoditu jsou 2 hodiny (celkem min. 10 hod), není-li uvedeno jinak. Školení bude probíhat v sídle zadavatele. Předpokládá se účast max. 3 osob.

2.5. Popis povinných parametrů dodávaného řešení

Komodita K1 – Virtualizační platforma		
Část	Parametr	Popis povinného parametru
Virtualizační server 1x	Provedení	rackové provedení max. 5U včetně výsuvných kolejnic a montážního materiálu do racku (datového rozvaděče). Maximální hloubka 60 cm pro umístění ve stávajícím racku.
	CPU	1x procesor, maximálně 16 jader Procesorový výkon dle https://spec.org/ minimálně: SPECrate®2017_int_base 108 bodů SPECrate®2017_fp_base 163 bodů
	RAM	Min. 128 GB, DDR5, min. 4800 MT/s, výkonově optimalizovaná konfigurace
	Úložiště pro hypervizor	Min. 2x SSD 480 GB, RAID1, nezabírá pozice HDD
	Úložiště	Min. 4x 1.9 TB SSD min. 1 DWPD, 3x 8TB 7200 ot./min, všechny s podporou výměny za provozu (hot-swap)
	Rozšiřitelnost	Min. 5 volných pozic HDD pro rozšíření kapacity, s možností osazení disků SATA/SAS. Všechny pozice aktivní, připojené k řadiči
	RAID hardware	SAS/SATA/NVMe řadič se zálohovanou vyrovnávací pamětí min. 8 GB. Podpora RAID 10,50 a 60 a HBA režimu.
	LAN	Porty min. 2x 1GbE, 4x 10/25 Gb SFP28 s podporou RDMA RoCEv2. Všechny NIC s podporou virtualizace – VMware NetQueue, Microsoft VMO. 1x 1GbE – samostatný port pro vzdálený management
	USB	min. 4x USB 3.2 porty, z toho min. 1x na čelním panelu s podporou bootování
	Management	Servisní modul s možností samostatného přístupu po management síti, možnost vzdálené klávesnice, myši a obrazovky bez nutnosti běhu OS, možnost zapínat a vypínat server, možnost bootování se vzdáleného média. Vyhrazený LAN port, podpora http/s, ssh, SNMP, syslog. Podpora vícefaktorového ověřování (autentizace) a integrace s Active Directory Standardizované REST API pro automatizaci. Monitorování spotřeby. HTML5 rozhraní
	Provozní podmínky	Určen a výrobcem podporován pro provoz v běžném neklimatizovaném prostředí min. do 35 stupňů Celsia
	Napájení	2x napájecí zdroj, redundance, min. Titanium specifikace dle 80 PLUS https://cs.wikipedia.org/wiki/80_Plus , dostatečný výkon pro plné osazení HDD
SW licence operačních systémů	Serverové operační systémy	2 ks licencí 64bitového serverového operačního systému v aktuální verzi. Každá licence musí umožnit provoz hypervizoru a 2 virtuálních serverů stejné verze v prostředí hypervizoru (serverové virtualizace), dále provoz Windows aplikací a všech nabízených aplikací a management nástrojů
	Klientské licence	Roční licence Microsoft 365 EDU A3 pro 50 zaměstnanců a min 600 studentů školy
	Terminálové licence	40 ks klientských licencí vázaných na uživatele pro využití funkcionality terminálových služeb (např. MS Remote desktop services) v nabízených operačních systémech
UPS 2x	Provedení	provedení do racku, max. 2U, včetně montážního materiálu
	Elektrické provedení	jmenovité napětí 230 V, jednofázová na vstupu i výstupu
	Výkon (VA/W)	3000 VA / 3000 W
	Technologie	online, dvojitá konverze
	Účinník	lepší než 0,98
	Stabilizace	výstupní napětí – odchylka max. ±5 % od jmenovité hodnoty
	Kapacita	dobu běhu na baterie min. 10 min při 50% zátěži
	Vstup	zásuvka IEC C14
	Výstupy	min. 8 zásuvek IEC C13, možnost omezení doby zálohování pro vybrané zásuvky (nekritická zařízení)
	Diagnostika	Vestavěný úplný systémový autotest, možnost automatického plánovaného provádění
	Servis	baterie musí být vyměnitelné za chodu
	Bypass	automatický interní bypass

Komodita K1 – Virtualizační platforma		
	Komunikační porty a rozhraní	RS-232, USB, LAN. SNMP a WEB rozhraní
	Stavové informace	stavový grafický displej pro konfiguraci a základní informace o stavu UPS
	Ochrany	inteligentní / optimalizované nabíjení pro optimalizaci výkonu a životnosti baterií, nastavení nabíjecího proudu
	Řízení	schopnost ovládání a restartování nabízeného serveru, korektní vypnutí operačních systémů
	SW kompatibilita	UPS musí být plně podporovaná výrobcem pro použití ve virtualizačních prostředích VMware a Microsoft Hyper-V, příslušný SW bude součástí dodávky
	Rozšiřitelnost	možnost prodloužení doby běhu na baterie připojením externích bateriových modulů min. na 30 minut
	Záruka	36 měsíců včetně baterií
SW licence zálohovací software (sada)	Licence	trvalá licence zálohovacího software pro všechny nabízené server bez omezení počtu zálohovaných virtuálních serverů a objemu dat.
	Efektivita ukládání dat	integrována komprimace a deduplikace
	Nároky na správu	„bezagentové“ řešení – bez instalace agentů do zálohovaných virtuálních serverů či aplikací
	Ochrana dat	provádění datově konzistentních záloh hlavních serverových aplikací – Active Directory, souborové systémy – bez nutnosti odstávky aplikace
	Optimalizace	využívání snapshotů, zálohování pouze dat (bloků virtuálního disku) změněných od poslední úspěšné zálohy
	Kompatibilita	podpora operačních systémů Windows a Linux v zálohovaných virtuálních serverech
	Uložiště záloh	možnost ukládání záloh na nabízený NAS
	Obnova	granulární obnova jednotlivých objektů včetně metadat (oprávnění, datum změny apod.), minimálně typu soubor
	Průvodci	vytváření a správa úloh (zálohování, obnova apod.) pomocí vestavěných průvodců včetně konfigurace automatického spouštění úloh
	Rychlá obnova	možnost spuštění virtuálního serveru přímo ze zálohy bez nutnosti obnovy na původní úložiště
	Kontrola záloh	možnost automatického ověření zálohy spuštěním zálohovaného virtuálního serveru
	Reporting	automatický reporting úspěšných i neúspěšných úloh
	Provedení	nevyžaduje licenci Windows server/desktop pro provoz serverové části aplikace
	Fyzické servery	podpora zálohování fyzických serverů nebo stanic bez omezení počtu (pro tuto funkci je přípustné využití agentů v zálohovaných systémech)
Sítové úložiště NAS 2 ks	Cloud	podpora zálohování prostředí Microsoft 365 (soubory, e-mailů atd.)
	Záruka	60 měsíců včetně nároku na opravné a nové verze
	Provedení	rackové provedení max. 2U včetně výsuvných kolejnic a montážního materiálu do racku. Maximální hloubka max. 40 cm pro montáž do stávajícího racku.
	Výkon	64 bit CPU, min. 4 jádra
	HDD	Min. 8 pozic pro HDD, rozšiřitelné min na 12 HDD
	Rozšiřitelnost	Podpora připojení externích disků přes USB 3 (min. 2 porty)
	Hot-swap	Disky vyměnitelné za chodu.
	SSD HDD	podpora SSD disků pro ukládání dat i akceleraci rotačních HDD
	Kapacita	Osazeno min. 8x 8TB HDD SATAIII/256MB cache, 7200 ot./min oficiálně podporovaných výrobcem NAS
	Konektivita	Min. 4 x 1 GbE a 2x 10Gb SFP+ porty s podporou agregace linek a redundance
	Výkon	Rychlost zápisu min. 1 000 MB/sec při RAID5 a SMB/CIFS v nabízené konfiguraci
	Kompatibilita	Plná podpora Microsoft Hyper-V a Windows Active Directory a ACL.
	Komunikace LAN	Sítové protokoly CIFS, WebDAV, iSCSI, SSH, SNMP, http/s
	UPS	Podpora korektního vypnutí signálem z UPS přes LAN při výpadku napájení
	RAM	min. 4 GB, využitelná jako cache. Rozšiřitelná min. na 16 GB
	Ochrana dat	Integrované typy ochrany dat RAID 1, RAID 5, RAID 6, RAID 10, integrovaný systém pro automatické vytváření a správu snapshotů (snímků dat), souborový systém Btrfs
	Záruka	60 měsíců včetně HDD

Komodita K2 – Zabezpečení LAN a WiFi		
Část	Parametr	Popis povinného parametru
Firewall 1x	Porty	min 8x 1GbE (min. 2x WAN) a 2x 10Gb SFP+, USB pro ext. modem
	NGFW	min. základní funkce Next-generation firewall – viz https://en.wikipedia.org/wiki/Next-generation_firewall - firewall, aplikační firewall s DPI, IPS. Administrace na bázi "objektů" (aplikace, uživatelů, lokality apod.) namísto IP adres, portů apod.
	Počet současných spojení	min. 1 000 000
	Propustnost SSL VPN	min. 1 Gbps, při licenčním nebo technickém omezení počtu klientů požadujeme min. 100 klientů
	Propustnost SSL inspekce	min. 2.5 Gbps
	Propustnost firewallu	min. 10 Gbps pro pakety 64 bytů a větší, provoz UDP
	Propustnost NGFW	min. 2.5 Gbps při aktivní IPS
	Propustnost IPS	min. 4 Gbps pro provoz typu Enterprise mix
	Propustnost detekce škodlivého kódu	min. 2 Gbps při zapnuté IPS
	Virtualizace	min. 5 virtuálních kontextů
	Vysoká dostupnost	režimy Active/Active se společnou konfigurací, včetně případných nezbytných licencí
	Dualstack	podpora současného běhu IPv4 a IPv6
	Aplikační kontrola	detekce, monitoring, povolení či zakázání obvyklých síťových aplikací na základě signatury dané aplikace, nikoliv dle portu Kontrola komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S,...)
	Antivir	integrovaný antivirus, podpora protokolu ICAP pro offload AV detekce, možnost detekce tzv. Grayware (rootkit, malware, spywave, keylogger, atd)
	Kategorizace a blokace provozu	založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorií na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorií jen po určitou dobu během dne
	Antispam	antispamová a antivirová inspekce elektronické pošty
	Sandbox	integrovaný sandbox (ověření škodlivosti kódu spuštěním v reálných operačních systémech) v zařízení nebo integrované rozhraní pro napojení na externí službu výrobce zařízení (služba součástí dodávky)
	Aktualizace	automatická aktualizace bezpečnostních funkcí poskytovaná výrobcem zařízení
	Ověřování uživatelů	LDAP, Active Directory, Single Sign On vůči Active Directory, Radius, Ověřování na základě certifikátu
	Management a monitoring	HTTP/S, SSH, SNMP, syslog,
	SD-WAN	integrovaná podpora SD WAN - min. rozkládání zátěže a vysoká dostupnost více internetových přípojek
Centrální přepínač 2x	Sledování toků	export síťových toků (Netflow nebo ekvivalent)
	Standardní funkce	NAT, statické a dynamické a routování, bezpečná publikace interních serverů
	Záruka	min. 60 měsíců v režimu 24x7 poskytovaná výrobcem zařízení. Odesláním náhradního zařízení max. následující den po nahlášení závady, včetně nároku na bezpečnostní aktualizace firmware a bezpečnostních funkcí – URL filtrace, IPS, antimalware, antispam, aplikační kontrola, sandbox)
	Základní parametry	L2/L3 přepínač v rackovém provedení max. 1U, neblokovaná architektura (přepínací kapacita min. 336 Gbps)
	Porty	48x 1GbE PoE+, 2x 10 Gb SFP+, 2x 40 Gb QSFP+
	PoE	podpora standardů IEEE 802.3af/at a podpora PoE+ na všech metalických portech, celkový PoE výkon min. 1400 W
	Agregace portů	podpora LACP, min. 20 portů v agregační skupině, bez omezení počtu skupin
	Směrování	hardwarové statické routování včetně VLAN, min. 16000 routovacích záznamů pro IPv4
Centrální přepínač 2x	Řízení provozu	víceúrovňový QoS, podpora standardu 802.1p
	VLAN	VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření, podpora IEEE 802.1ad (Q-in-Q), min. 4000 VLAN

Komodita K2 – Zabezpečení LAN a WiFi		
	Ověřování uživatelů a zařízení	plná podpora 802.1X
	Dualstack	plný IPv4 a IPv6 dualstack včetně směrování a QoS
	MAC	podpora min. 30 000 MAC adres
	Síťové toky	plný přímý export síťových toků – Netflow, IPFIX nebo ekvivalent (sFlow není ekvivalent)
	Zrcadlení portů	podpora RSPAN (Remote SPAN) a ERSPAN (Encapsulated Remote SPAN)
	Monitoring a správa	plná podpora CLI, SSH, SNMP, syslog, sFlow, web rozhraní, REST nebo SOAP/WDSL API pro automatizaci (např. z IDM)
	Nezávislý management	vyhrazený samostatný síťový port pro management (nezapočítává se do požadovaného počtu portů)
	Napájení	Interní redundantní napájecí zdroje vyměnitelné za provozu (hot-swap)
	Centrální správa	jednotná centrální správa, monitorování a aktualizace firmware z centrální grafické konzole obsažené ve firmware nabízených síťových prvků.
	Stohování	pokročilé stohování s rozložením LAG (link aggregation group) mezi více přepínači ve stohu - např. technologie MLAG (Multi-Chassis Link Aggregation) nebo obdobná
	Záruka	min. 60 měsíců poskytovaná výrobcem zařízením, včetně opravných verzí firmware
Přístupový přepínač 3x	Společné parametry	
	Základní parametry	L2+ přepínač v rackovém provedení max. 1U a hloubka do 32 cm, neblokovaná architektura
	Agregace portů	podpora LACP, min. 8 portů v agregační skupině, min. 12 skupin
	Směrování	statické routování
	Řízení provozu	víceúrovňový QoS, podpora standardu 802.1p
	VLAN	VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN na základě 802.1X ověření
	Ověřování uživatelů a zařízení	plná podpora 802.1X
	Dualstack	plný IPv4 a IPv6 dualstack včetně směrování a QoS
	MAC	podpora min. 30 000 MAC adres
	Síťové toky	plný přímý export síťových toků – Netflow, IPFIX nebo ekvivalent (sFlow není ekvivalent)
	Monitoring a správa	plná podpora CLI, SSH, SNMP, syslog, sFlow, web rozhraní, REST nebo SOAP/WDSL API pro automatizaci (např. z IDM)
	PoE	pro PoE provedení podpora standardů IEEE 802.3af/at
	Centrální správa	jednotná centrální správa, monitorování a aktualizace firmware z centrální grafické konzole obsažené ve firmware nabízených síťových prvků.
	Zrcadlení portů	podpora SPAN
	Hlučnost	max hlučnost 43/47 dB (nePoE/PoE varianty) pro umístění v pracovních prostorech
	Záruka	min. 60 měsíců poskytovaná výrobcem zařízením, včetně opravných verzí firmware
WiFi přístupový bod vnitřní 27 ks	Specifické parametry	
	Počty, porty a propustnost, PoE výkon (budget)	2x přístupový přepínač – 48x 1 Gb RJ-45 PoE + 4x 10 Gb SFP+, 176 Gbps, min. 370W 1x přístupový přepínač – 48x 1 Gb RJ-45 + 4x 10 Gb SFP+, 176 Gbps
	Základní funkce	Přístupový bod (AP) standardu WiFi6 včetně montážního materiálu na strop
	Frekvence	min. 3 nezávislé radiové moduly činnost v radiovému pásmu 2,4 a 5 GHz současně, s podporou standardu OFDMA min. u 2 modulů
	Architektura	Homegení WiFi síť s rychlým a spolehlivým roamingem klientů, podpora Mesh (https://en.wikipedia.org/wiki/Wireless_mesh_network)
	Anténní systém	interní systém, optimalizovaný pro montáž na strop
	Současná obsluha více klientů	Podpora MU–MIMO (Multi–User MIMO) – multi–user multiple input/multiple output
	Přenosové rychlosti	5GHz min 1200 Mbps, 2.4 GHz min. 550 Mbps
	Standardy	podpora standardů 802.3at, 802.11n, 802.11ax, 802.11k, 802.11n, 802.11r, 802.11v, Hotspot 2.0
	Multi SSID	podpora vysílání min. 8 SSID (WiFi sítě) na 2.4 i 5 GHz současně, podpora přiřazení každého SSID do samostatné VLAN
	Zatížení	min. 300 přiřazených (asociovaných) klientů na radiový modul

Komodita K2 – Zabezpečení LAN a WiFi		
	Řízení zátěže	automatické rozkládání zátěže přístupových bodů předáváním klientů a automatickým směrováním klientů na 5 GHz (pokud klienti podporují)
	Porty	min. 2x 1Gb, min 1x PoE s podporou standardů 802.3at a 802.3af
	Bezpečnost	trvalá detekce cizích přístupových bodů/klientů nezávislým radiem, spektrální analýza
	Kontroler	centrální kontroler pro kompletní centrální správu WiFi infrastruktury a řízení jejího provozu včetně roamingu klientů součástí dodávky. Kontroler musí být provozován v interní síti zadavatele (nezávislý na cloudu) a být integrální součástí firmware nabízených síťových prvků.
	Autentizace, autorizace	podpora standardu WPA3 (WiFi Protected Access III), integrovaný portál pro autentizaci uživatelů (Captive portal), ověření klientů (min. hardware, uživatel, operační systém, certifikát) s využitím protokolu 802.1X
	IoT a lokalizace	integrovaná hardwarová podpora standardu 802.15.4 (Zigbee) a BLE (Bluetooth Low Energy)
	Správa	plná podpora CLI, SSH, SNMP, syslog, web rozhraní, hromadná aktualizace firmware a konfigurace
	Monitoring	detailní monitoring a diagnostika provozu v reálném čase – parametry připojení a komunikace klienta, stav přístupových bodů (počty klientů, vytížení kanálů, signál, cizí (rogue) přístupové body)
	Úsporné napájení	podpora standardu 802.3az – Energy-Efficient Ethernet (EEE)
Licence síťových prvků	Záruka	min. 60 měsíců poskytovaná výrobcem zařízením, včetně opravných verzí firmware
	Licence	Licence pro využití veškerých požadovaných funkcionalit síťových prvků (firewall, přepínače, přístupové body), pokud nabízené řešení takové licence vyžaduje.
Příslušenství síťových prvků	Podpora a platnost	min. 60 měsíců poskytovaná výrobcem
	SFP moduly	14 ks modulů SFP+ 10 Gb, SM min. 1 km, WDM (BiDi), včetně DMI diagnostiky pro nabízené přepínače, LC konektor (7 párů – komplementární frekvence) 4 ks modulů SFP+ 10 Gb, SM min. 1 km, včetně DMI diagnostiky pro nabízený NAS, LC konektor 1x kabel DAC 40 Gbps QSFP+ 1 m pro nabízené přepínače 2x kabel 40 Gbps 1xQSFP+ - 4xSFP+, 5 m pro nabízené přepínače a servery
	Patch kabely	12 ks optický kabel SM s konektory LC-SC, simplex, 2 m 8 ks optický kabel SM s konektory LC-SC, 2 m 8 ks optický kabel SM s konektory LC-SC, 5 m
	Záruka	min 36 měsíců

Komodita K3 – Centrální logování a Správa identit		
Část	Parametr	Popis povinného parametru
Systém pro sběr a správu logů 1x	Základní funkce	systém pro sběr, ukládání a správu provozních a bezpečnostních informací a událostí ze sledovaných systémů
	Protokoly sběru logů	syslog, TCP, UDP, HTTP, JSON
	Sběr síťových toků	Netflow či kompatibilní dle nabízeného firewallu a přepínačů
	Zdroje logů	min. REST API, textové soubory, Radius, Active Directory, MS SQL databáze, Windows Event Log – včetně rozšířených "Applications and Services Logs", síťové prvky – syslog a Netflow, ostatní aktivní prvky – syslog, SNMP trap, Office 365, Sysmon (Windows)
	Parsování logů	integrovaný nástroj pro parsování logů. Možnost nahrání části logu, online vytváření parseru a snadné testování výsledku. Podpora vytváření opakovaně použitelných vzorků - např. definice IP adresy regulárním dotazem apod.
	Retence	uchovávání logů min. 6 měsíců, automatická retence logů a indexů
	Geolokace	podpora automatické doplňování logů o informaci o lokalitě podle IP adresy
	Normalizace logů	sjednocení názvů shodných dat z různých zdrojů logů např. pro snadné vyhledávání napříč zdroji
	Rozšíření logů	podpora rozšíření logů o vlastní statické a dynamické (kalkulované) položky integrovaným nástrojem.
	Bezpečnost	podpora šifrované komunikace se zdroji (SSL apod.), ověřování zdrojů (TLS apod.)
	Výkon	min. 1000 EPS (event per second), 5000 FPM (flows per minute)
	Dashboardy	uživatelské vytváření dashboardů (pracovních desek) včetně možnosti využití grafických prvků (grafy, mapy, histogramy apod.) i strukturovaných dat (tabulek)
	Export dat	export dat do csv nebo jiného strojově čitelného formátu - min. výsledky hledání

Komodita K3 – Centrální logování a Správa identit		
	Kanály	možnost vytváření kanálů – datových sad či toků – na základě pravidel (logických podmínek) a to i napříč různými zdroji. Podpora dalšího zpracování – tvorba alarmů, zobrazení na dashboardu, online odesílání do nadřazeného systému apod.
	Výstrahy, upozornění	podpora vytváření výstrah – překročení okamžitých či kumulovaných hodnot, zasílání upozornění
	Active Directory	integrace s Active Directory pro ověřování uživatelů, nastavení oprávnění min. administrátor a operátor
	Vyhledávání	rychlé a intuitivní vyhledávání v záznamech napříč všemi zdroji i při velkých objemech dat (řády TB). Jednoduchý dotazovací jazyk. rychlá vyhledávání či filtrování bez tvorby dotazů - např. výběrem v kontextovém menu vybraného pole uloženého záznamu.
	Ovládání	intuitivní grafické webové rozhraní dostupné z běžných prohlížečů (Edge, Chrome, Firefox)
	Integrace	podpora integrace s Windows OS v úrovni sledování spuštěných příkazů (cmd, powershell), vyvážení procesů, změny souborů, registrů a síťové komunikace. Včetně nástrojů pro detekci potenciálně nebezpečných aktivit (změna časových razítek souborů apod.)
	Detekce zranitelnosti	automatická kontrola zranitelnosti operačních systémů Windows, Linux a macOS a aplikací (host based vulnerability detection)
	Detekce škodlivého kódu	automatická kontrola výskytu škodlivého kódu (malware, rootkity, neobvyklé chování) v monitorovaných operačních systémů Windows, Linux a macOS
	Hodnocení zabezpečení	automatické kontrola konfigurací a nastavení monitorovaných operačních systémů Windows, Linux a macOS a aplikací, hodnocení úrovně zabezpečení monitorovaného systému
	Kompatibilita	podpora provozu v prostředí serverové virtualizace Hyper-V
	Ukládání dat	do databáze, případná databázová licence musí být součástí dodávky
	Výstupy	možnost výstupů do nadřazeného systému pro účely vzdáleného expertního dohledu. Zabezpečený přenos vhodným protokolem
	Záruka	min. 60 měsíců včetně poskytnutí opravných verzí
Systém pro správu identit (Identity management – IDM) včetně API/integračních modulů 1x	Základní funkce	IDM (dále IDM nebo Systém) bude udržovat a spravovat identity a organizační strukturu organizace – třídy, učitelský sbor, administrativa atd. Spravované identity budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy. Identity budou ukládány v databázi. Systém bude spravovat i identity externích uživatelů (spolupracovníků a partnerů) využívajících ICT systémy zadavatele.
	Licence	trvalá licence, která 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.). Předpokládaný počet spravovaných identit je min. 1500
	Uživatelské rozhraní	uživatelské rozhraní bude realizováno jako webový portál (dále jen Portál) dostupný z běžných prohlížečů (Edge, Chrome, Firefox) a umožní přístup k datům a funkcím Systému i jeho správu a konfiguraci.
	Evidence aplikací a rolí	integrováný registr aplikací a informačních systémů (souhrnné IS) a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby a zařazování uživatelů do rolí v příslušných IS
	Historizace	vestavěná detailní databázové historizace pro evidenci změn identit včetně referenčních objektů a vazeb mezi nimi. Historizace poskytne data v libovolném časovém okamžiku – aktuálním nebo zpětně v minulosti.
	Automatizace	podpora tvorby pravidel v grafickém prostředí pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě libovolných atributů identity a přidružených referenčních objektů (třída, organizační jednotka, aplikační role, pracovní pozice atd.).
	Logování	integrování logování min. následujících typů událostí: - události systému včetně webových služeb (aplikační log) - změny entit evidovaných systémem a změny konfigurace systému (auditní log) - synchronizace s napojenými systémy (synchronizační log) - odeslané notifikace a upozornění (notifikační log) Logy musí být dostupné nabízenému logovacímu systému nebo do něj exportovány
	Referenční objekty	systém umožní přidávání a správu libovolných typů referenčních objektů, a to i v průběhu správy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity. Základní (předpřipravené) referenční typy objekty budou min. pracovní pozice, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role.
	Popisné atributy	systém umožní dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IDM.
	Zobrazení	portál umožní grafické zobrazení a současné vyhledávání identit / uživatelských účtů ve stromové organizační struktuře a prohledávání organizační struktury včetně pracovních pozic až do úrovně jednotlivých uživatelských účtů (identit).

Komodita K3 – Centrální logování a Správa identit		
	Aktivní uživatelé	systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem
	Slučování identit	systém umožní sjednocení více uživatelů (identit) do jedné a odpovídající sjednocení spravovaných účtů.
	Oprávnění	víceúrovňová správa administrátorských oprávnění s možností nastavení oprávnění min. na úrovni organizační jednotky (nebo hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení pracovní pozice, přiřazení aplikační role, editace identity apod.)
	Časová omezení	IDM bude umožňovat přiřazení rolí konkrétní identitě, pracovní pozici, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení platnosti přiřazení. Po vypršení platnosti přiřazení IDM rolí přiřazenému objektu automaticky odebere.
	Vícenásobné vazby	možnost přiřazení identit k pracovním pozicím ve vazbě M:N. Identita může být v IDM evidována na více pracovních pozicích současně a současně na pracovní pozici může být evidováno více identit.
	Přehled rolí	možnost zobrazení přidělených rolí k jednotlivým identitám s přehledným rozlišením rolí navázaných na pracovní pozici, rolí navázaných na identitu, rolí navázaných na organizační jednotku, rolí navázaných na skupinu a delegovaných role.
	Přehled dědičností	IDM umožní evidenci a přehledné souhrnné zobrazení všech rolí včetně informace, odkud uživatel roli zdědil (z organizační jednotky, pracovní pozice, skupiny) nebo zda má nějakou roli od někoho delegovanou.
	Obnovení hesla	IDM bude obsahovat samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zaslání kódů pro reset hesla danému uživateli musí být možno provádět min. pomocí SMS (tj. IDM musí být možné na SMS bránu či službu napojit). Rozhraní musí umožnit i běžnou změnu hesla (bez resetu).
	Individualizace	IDM umožní uživatelům individuálně nastavit vlastní zobrazení rozhraní – min. zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku – vždy pro každý seznam samostatně.
	Upozornění	IDM zajistí zaslání konfigurovatelných emailových upozornění min. pro následující události: vytvoření a změna identity, referenčního objektu (pracovní pozice, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role atd.), problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu.
	Šablony upozornění	šablony upozornění umožní definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám musí být možné nastavovat různé příjemce pro různé části organizační struktury (např. třída, oddělení) apod. Šablony musí umožnit vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu.
	Bezpečnost změn	veškeré změny vyvolané požadavky uživatele a administrátorů/správců IDM budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v identitách a referenčních objektech i v administraci a konfiguraci IDM. Záznam v logu bude obsahovat původní i novou hodnotu.
	Důvěryhodnost	veškeré požadavky na změny v IDM bude možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových souborů jako XML, CSV atd. z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM.
	Auditní report	IDM umožní export auditního reportu z údajů o identitách uložených v IDM, a to i historických. Auditní reporty budou minimálně ve formátu XML nebo CSV a budou obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IDM, pracovních pozic, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti. Filtrování reportovaných identit musí být možné podle libovolných atributů identity včetně přidružených referenčních objektů
	Standardy WS	systém bude disponovat aplikačním rozhraním (API) webových služeb, které budou definované v rozšířeném standardu WSDL a podporovat protokol SOAP.
	Bezpečnost WS	konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně.
	Synchronizace	ruční i automatické spuštění synchronizací s propojenými systémy. Musí být implementovány minimálně následující typy synchronizací: - Plná synchronizace – prochází všechny objekty v IDM a synchronizuje je s odpovídajícími objekty daného systému - Změnová synchronizace – synchronizuje jen změny od poslední provedené synchronizace. - Simulační synchronizace – synchronizace vytvoří report očekávaných změn v napojeném systému (bez ovlivnění produkčních dat). Průběh a výsledek všech synchronizací bude dostupný v přehledné podobě v grafickém prostředí Portálu
	Historie synchronizací	záznam běhů synchronizací v historii dostupné v Portálu. Historie plné synchronizace bude obsahovat odkazy na objekty, které byly synchronizovány a log, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak bude v historii dále informace o události, která změnovou synchronizaci vyvolala.
	Správa synchronizací	správa jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, nastavení časového intervalu spouštění, nastavení intervalu odstavky a výběru synchronizované organizace bude součástí Portálu.
	Zdrojový systém	IDM bude napojen na školský informační systém Škola OnLine https://www.skolaonline.cz/ . Ze systému budou načítány údaje o organizační struktuře, osobách a tyto údaje budou pro IDM sloužit jako zdrojové
	Aplikační moduly/konektory	IDM bude spravovat identity a řídit oprávnění v dále vyjmenovaných systémech. V těchto systémech bude IDM vytvářet a aktualizovat uživatelské účty, nastavovat jejich oprávnění k rolím a (v prostředí cloudu) přiřazovat licence - Microsoft Active Directory

Komodita K3 – Centrální logování a Správa identit		
		- Microsoft 365 - obecný – simulace aplikace, požadavky na změny IDM zasílá e-mailem správci aplikace, který je jich provedení potvrzuje zpět v IDM pro účely evidence změn a logování
	Záruka	60 měsíců včetně nároku na opravné verze

Komodita K4 – Koncová zařízení		
Část	Parametr	Popis povinného parametru
Koncové zařízení – stolní počítač 34x	Provedení	Formát SFF nebo menší
	CPU	výkon CPU dle https://www.cpubenchmark.net min. 23 500 bodů
	Video	výkon video/grafického procesoru dle https://www.videocardbenchmark.net min. 1750 bodů
	RAM	16 GB DDR5, rozšiřitelná min. na 32 GB bez výměny modulů
	HDD	min. 500 GB SSD, provedení PCIe NVMe
	LAN	1 Gb, standardní RJ-45 port
	Bezdrátové připojení	min. WiFi 6, IEEE 802.11ax, 2.4 + 5 GHz, anténní systém MIMO 2x2 pro vysokou propustnost Bluetooth min. 5.2
	Porty	Čelní panel - min. 3x USB, z toho min 1x USB Type-C 20 Gb/s, ostatní Type-A nebo Type-C min. 10 Gb/s, audio – sluchátka a mikrofon Zadní panel - min. 2x DisplayPort 1.4, 1x HDMI 1.4, min. 3x USB 10 Gbps Type-A nebo Type-C
	Periferie	USB klávesnice se samostatným numerickým blokem a českým popisem USB optická myš
	Bezpečnost	TPM 2.0 čip
	Audio	integrováný reproduktor
	Software	Operační systém Microsoft Windows v aktuální verzi s podporou domény Active Directory, 64-bitový, české rozhraní Požadavky na software jsou dány kompatibilitou se stávajícím prostředím a pořízeným výukovým programovým vybavením.
	Záruka	min. 60 měsíců poskytovaná výrobcem, oprava následující pracovní den v místě instalace
Koncové zařízení – stanice pro správu 1x	Provedení	Formát SFF
	CPU	výkon CPU dle https://www.cpubenchmark.net min. 37 500 bodů
	Video	výkon video/grafického procesoru dle https://www.videocardbenchmark.net min. 1750 bodů
	RAM	32 GB DDR5, rozšiřitelná min. na 64 GB bez výměny modulů
	HDD	min. 1 TB SSD, provedení PCIe NVMe a 1x 3.5" volný interní slot pro SATA HDD
	LAN	1 Gb, standardní RJ-45 port
	Bezdrátové připojení	min. WiFi 6, IEEE 802.11ax, 2.4 + 5 GHz, anténní systém MIMO 2x2 pro vysokou propustnost Bluetooth min. 5.2
	Porty	Čelní panel - min. 5x USB, z toho min 1x USB Type-C 20 Gb/s, ostatní Type-A nebo Type-C min. 10 Gb/s, audio – sluchátka a mikrofon Zadní panel - min. 2x DisplayPort 1.4, 1x HDMI 1.4, min. 6x USB Type-A nebo Type-C, audio in/out
	Sloty	min. 1x PCIe Gen4 x16, 1x PCIe x4, 1x PCIe x1
	Periferie	USB klávesnice se samostatným numerickým blokem a českým popisem USB optická myš
	Bezpečnost	TPM 2.0 čip
	Audio	integrováný reproduktor
	Software	Operační systém Microsoft Windows v aktuální verzi s podporou domény Active Directory, 64-bitový, české rozhraní Požadavky na software jsou dány kompatibilitou se stávajícím prostředím a pořízeným výukovým programovým vybavením.
	Záruka	min. 60 měsíců poskytovaná výrobcem, oprava následující pracovní den v místě instalace
Monitor	Provedení	27", tenký rámeček, matný – antireflexní povrch, VESA montážní standard

Komodita K4 – Koncová zařízení		
1x	Panel	technologie IPS, podsvícení LED, odezva do 5 ms, min 75 Hz
	Rozlišení	QHD (2560 x 1440)
	Porty – video	min. 2x DisplayPort (vstup/výstup), 1x HDMI, USB-C, včetně DisplayPort kabelu pro připojení k počítači
	Porty – data	min. 3x USB Type-A včetně kabelu pro připojení k počítači min. 2x USB Type-C, z toho min. 1x podpora Power Delivery min 60 W a LAN 1x Ethernet 1Gb
	Nastavení polohy	Výškově stavitelný, otočný kolem svislé osy, nastavitelný sklon, otočný na výšku (PIVOT)
	Záruka	min. 36 měsíců poskytovaná výrobcem, oprava následující pracovní den v místě instalace
Koncové zařízení – notebook 30x	Provedení	Notebook určený pro pracovní použití (ne domácí / herní apod.), hmotnost do 2 kg
	Displej	velikost 15-16", rozlišení FullHD (min. 1920 x 1080), provedení IPS, antireflexní
	CPU	výkon CPU dle https://www.cpubenchmark.net min. 16 000 bodů
	Video	výkon video/grafického procesoru dle https://www.videocardbenchmark.net min. 2550 bodů
	RAM	min. 16 GB DDR4
	HDD	min. 500 GB SSD, provedení PCIe NVMe
	LAN	1 Gb, standardní RJ-45 port
	Bezdrátové připojení	min. WiFi 6, IEEE 802.11ax, 2.4 + 5 GHz, anténní systém MIMO 2x2 pro vysokou propustnost Bluetooth min. 5.2
	Porty	min. 2x USB Type-C s podporou Power Delivery (PD) a DisplayPort min. 2x USB Type-A min. 1x HDMI min. 1x audio (mikrofon/sluchátka)
	Kamera	min. 720p
	Bezpečnost	integrovaný čip TPM 2.0 a čtečka otisků prstů
	Audio	integrované stereo mikrofony a reproduktory
	Klávesnice	podsvícená klávesnice se samostatným numerickým blokem a touchpadem. České rozložení kláves
	Napájení	včetně baterie (min. 40Wh) a odpovídajícího napájecího adaptéru
Úložná a nabíjecí stanice notebooků	Software	Operační systém Microsoft Windows v aktuální verzi s podporou domény Active Directory, 64-bitový, české rozhraní Kancelářský balík Microsoft Office Standard v aktuální verzi, české rozhraní Požadavky na software jsou dány kompatibilitou se stávajícím prostředím a pořízeným výukovým programovým vybavením.
	Záruka	min. 60 měsíců poskytovaná výrobcem, oprava následující pracovní den v místě instalace
	Provedení	pevný kovový box pro uložení a současné nabíjení všech 30 nabízených notebooků.
	Větrání a napájení	aktivní větrání integrovanými ventilátory, vestavěné jištění nadproudu (přetížení) a proudový chránič. Centrální vypínač, světelná indikace zapnutého stavu
	Bezpečnost	uzamykatelný box, vícebodové uzamykání
	Nabíjení	min 30 standardních zásuvek 230 V s ochranným kolíkem pro napájecí adaptéry, min. 30 nabíjecích USB portů 5V / 2A
	Manipulace	otočná pojezdová kolečka s aretací, hlavní dvířka s velkým úhlem otevírání min. 170°, madla pro bezpečné uchopení při manipulaci
	Rozměry	max. 1300 x 900 x 700 mm (V x Š x H)
	Záruka	Min. 24 měsíců

Komodita K5 – Kabelové rozvody LAN		
Část	Parametr	Popis povinného parametru
Kabelové rozvody včetně příslušenství	Popis	Kabelové rozvody včetně příslušenství a souvisejících služeb dle podrobného výkazu výměr – Kapitola 4 - Výkaz výměr
	Záruka	Kabelové rozvody 10 let

3. Záruky a servisní podmínky

3.1. Požadavky na záruky a servisní podmínky

- (1) Zadavatel uvádí u jednotlivých komodit požadovanou min. záruku, záruční servis a podporu. V případě, že není hodnota výslovně uvedena, požaduje zadavatel standardní záruku v délce 24 měsíců s odstraněním vady nebo náhradou zařízením novým do 30 kalendářních dnů od nahlášení vady v místě plnění.

Z důvodu zajištění udržitelnosti projektu a zajištění bezpečnosti provozu po dobu 60 měsíců požaduje zadavatel poskytnutí prodloužených záruk pro některé komponenty, v jejichž popisu je informace o prodloužené záruce uvedena, při zachování ostatních parametrů původní záruky (rychlost opravy, rozsah aktualizací firmware apod.). Cenu tohoto prodloužení zahrne dodavatel pro tyto položky v Kalkulaci nabídkové ceny (viz. **Příloha č. 4 zadávací dokumentace, list „Provoz“**) do samostatných řádků označených vždy názvem položky a upřesněním prodloužené záruky. Tyto požadavky do 12. měsíců od pořízení jsou oceněny v rámci nabídkové ceny za jejich pořízení viz. **Příloha č. 4 zadávací dokumentace, list „Pořízení“**). Obdobně bude vyčíslen záruční servis u komponent, u kterých je požadován. Tyto náklady je nutné vyčíslit zvlášť, z důvodu financování udržitelnosti projektu. Zadavatel v rámci této technické specifikace požaduje specifické služby, které se odvíjejí od konkrétního typu plnění, a to zejména následující:

- záruka – záruku v intencích zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů, tedy, že si předmětné plnění po dobu záruky zachová své vlastnosti a parametry z doby dodávky a dále, že po celou dobu záruky bude mít parametry a vlastnosti požadované objednatelem;
 - prodloužená záruka – jedná se o záruku v intencích výše uvedené odrážky „záruka“ na dobu delší než standardní nebo obvyklou za dodržení parametrů a požadavků na záruku zařízení;
 - záruční servis – záruční servis v parametrech konkrétního SLA (service level agreement) uvedeného u každého jednotlivého zařízení, u kterého je záruční servis požadován; předmětem záručního servisu je zajištění podpory provozu a odstraňování závad dodaných zařízení dodavatelem nebo výrobcem zařízení s garancí po požadované dobu;
 - podpora – u části plnění spočívající v dodávce software a jejich licencí, kde není relevantní požadovat záruku ani záruční servis, požaduje objednatel technickou podporu daného software po dobu stanovenou vždy u konkrétního softwarového produktu; primární součástí takové podpory musí být nárok na opravné verze software a přístup k řešení problémů s takovým software, další specifické požadavky podpory jako nárok na veškeré nové verze nebo další požadavky jsou vždy konkrétně uvedeny u předmětné podpory a konkrétního software v této technické specifikaci.
- (2) Zadavatel požaduje bezplatný (zahrnutý v ceně zakázky) přístup k aktualizacím software a firmware dodaných komodit minimálně po dobu záruky.
- (3) Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro zadavatele.
- (4) Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.
- (5) 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.

Pro hlášení servisních požadavků zajistí dodavatel zadavateli přístup ke svému helpdeskovému systému s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení. Detailní popis helpdeskového systému a jeho obsluhy musí být součástí předávacích dokladů při předání díla. Provozní doba helpdeskového systému musí být minimálně 8–17 hod. v pracovních dnech.

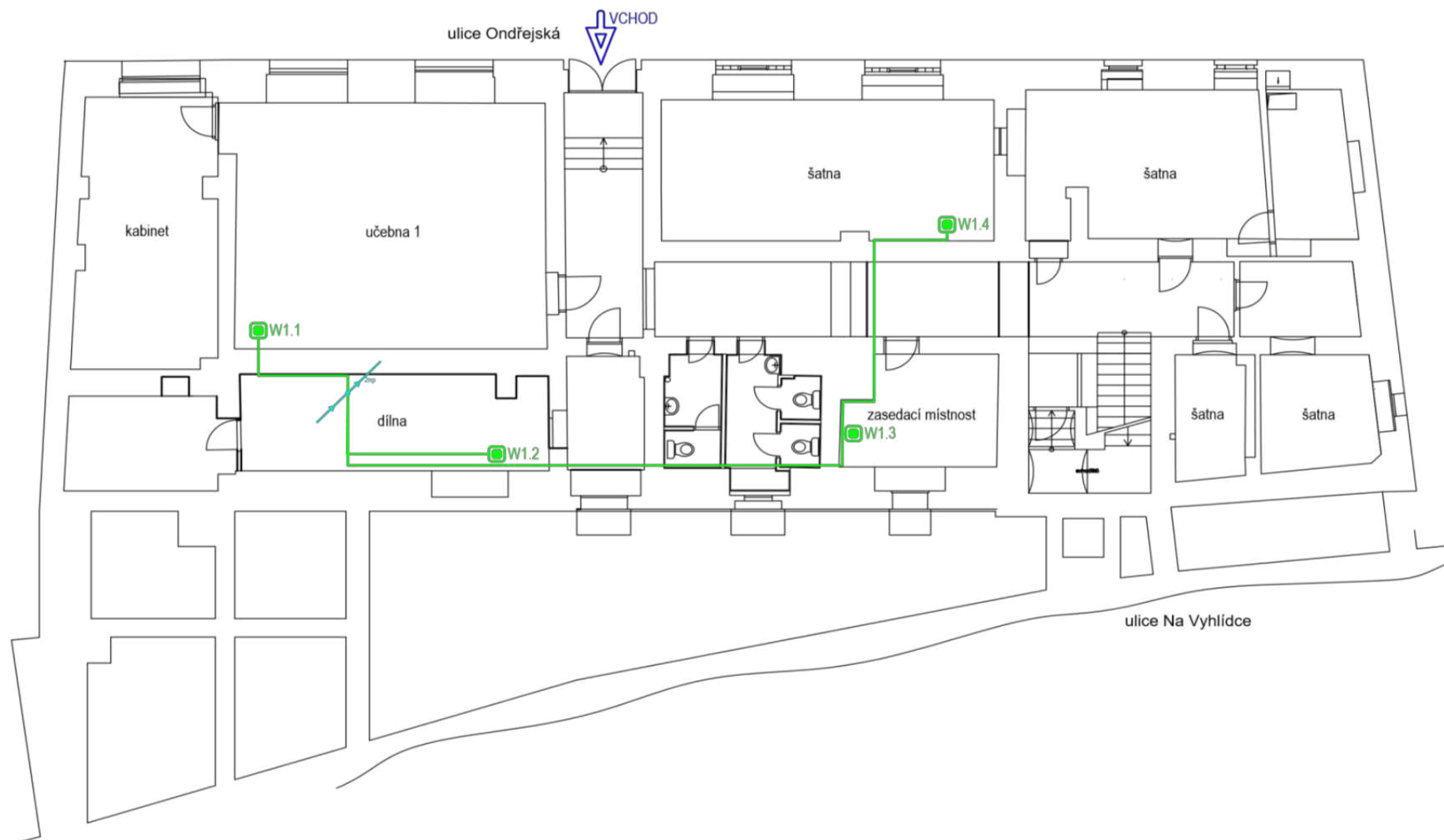
4. Specifikace síťových kabelových rozvodů a specifikace datových rozvaděčů

V ceně položky označené v **Kalkulaci nabídkové ceny** (viz. Příloha č. 4b zadávací dokumentace) komodity **K5 – Kabelové rozvody LAN** jako „**Kabelové rozvody včetně příslušenství**“, jsou zahrnuty dílčí položky specifikované v samostatné kalkulaci (dokument nazvaný – **P4a_Položkový soupis slaboproudých rozvodů k ocenění**). Dodavatel v **Kalkulaci nabídkové ceny** oceňuje kabelové rozvody včetně příslušenství a datových rozvaděčů jako celek. Položkový soupis kabelových rozvodů k ocenění slouží dodavateli pro kalkulaci celkové ceny této položky. **Cena kabeláže v položce Kabelové rozvody včetně příslušenství v Kalkulaci nabídkové ceny musí být totožná s celkovou cenou uvedenou v Položkový soupis slaboproudých rozvodů k ocenění.**

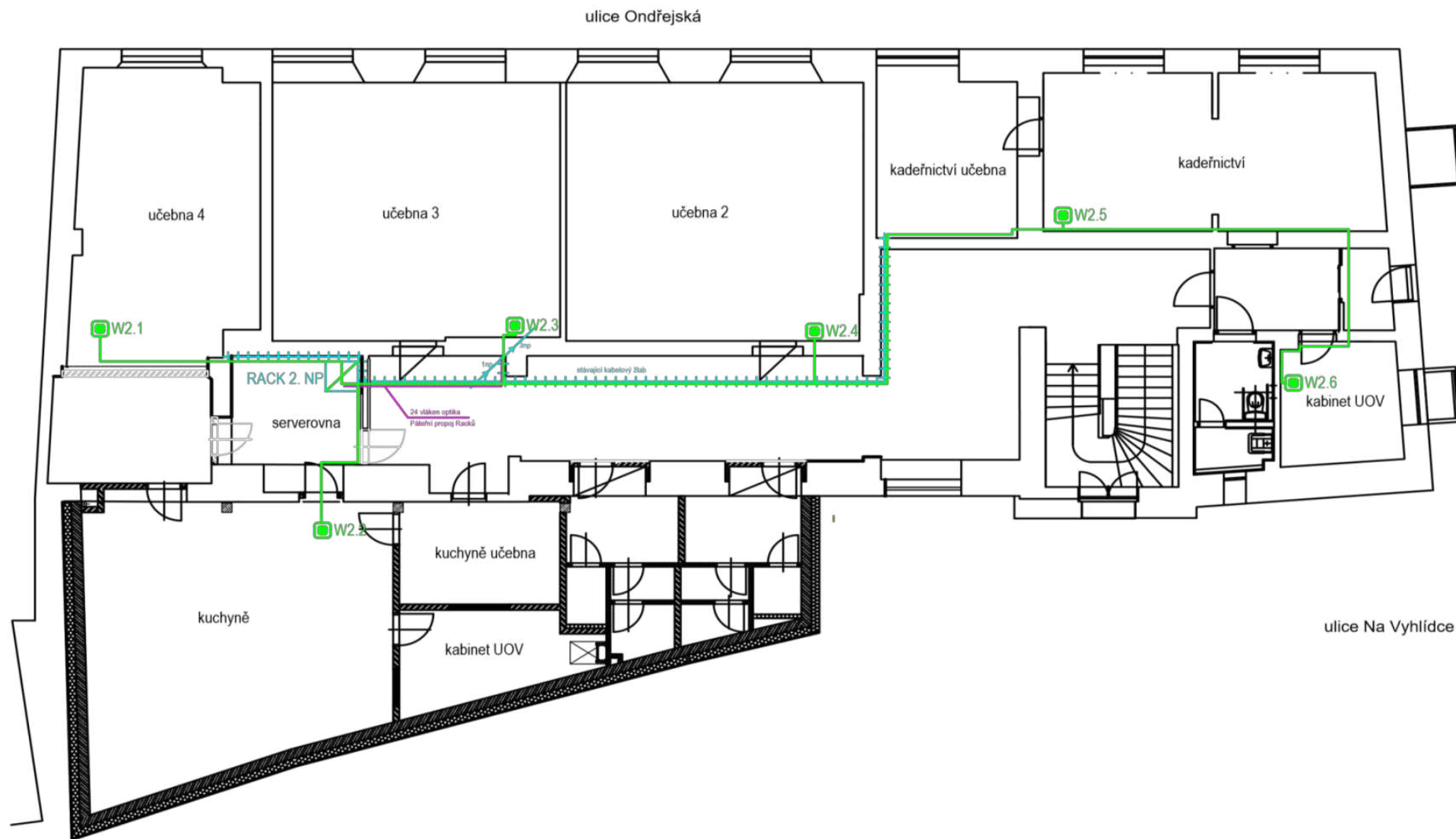
Dodavatel nacenění provede včetně záruky na kabelové rozvody v délce 10 let.

Požadované provedení kabelových rozvodů je uvedeno v projektové dokumentaci, kterou tvoří příloha č. 2b zadávací dokumentace.

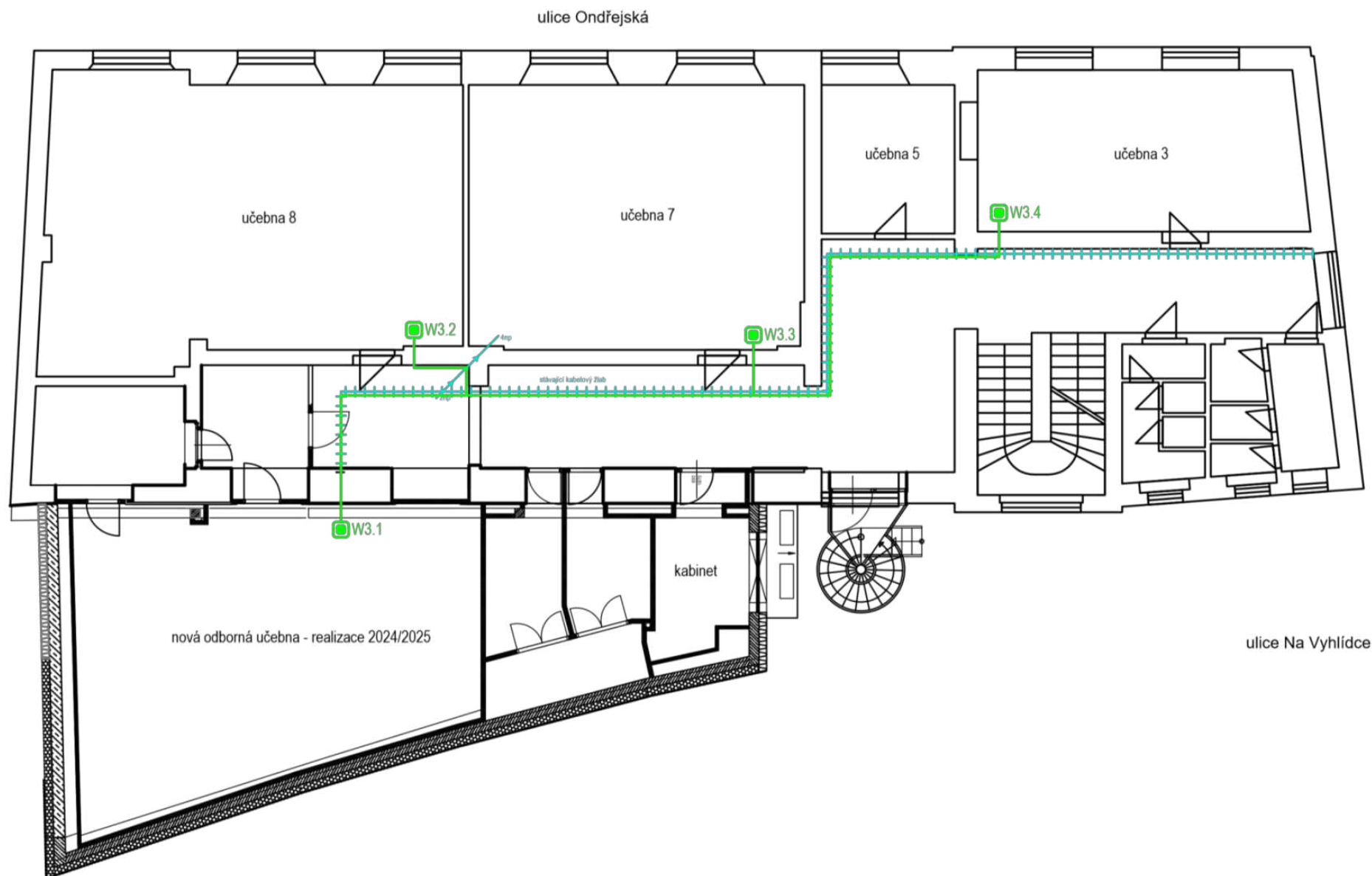
4.1. Plány požadovaného provedení



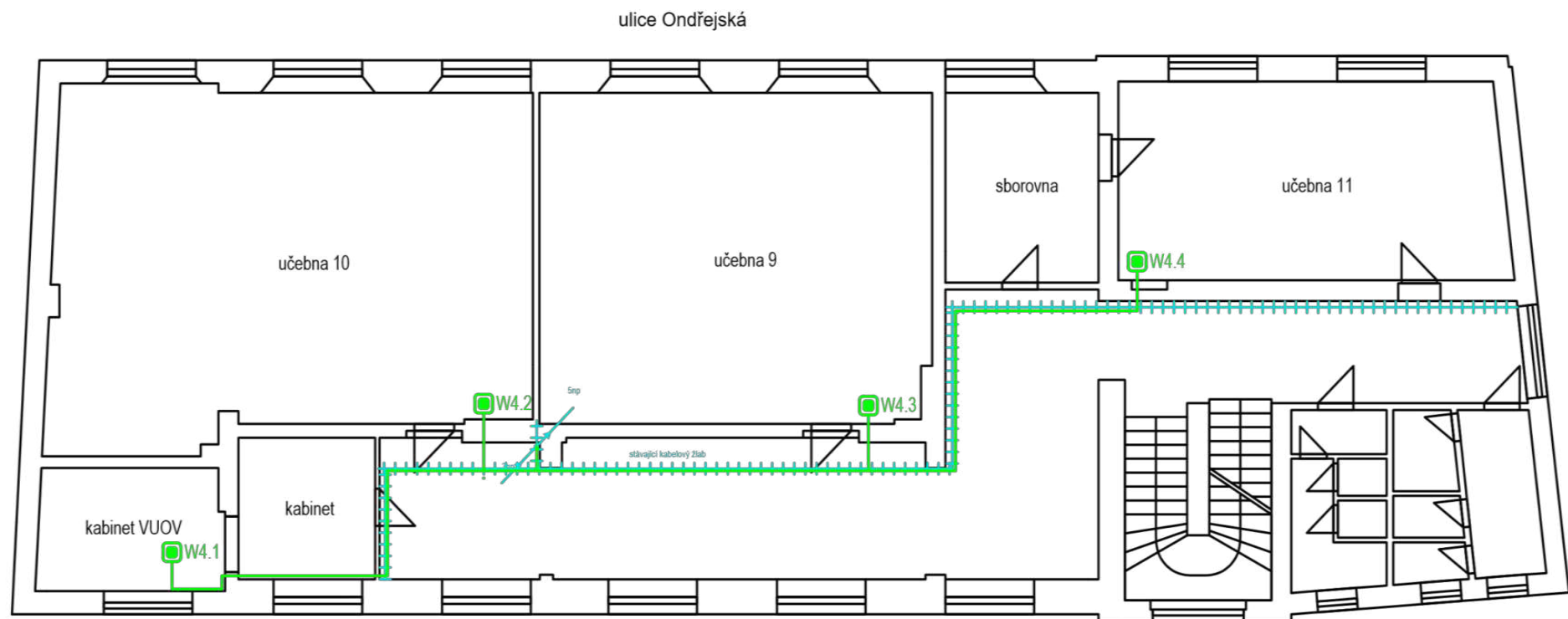
1. nadzemní podlaží



2. nadzemní podlaží

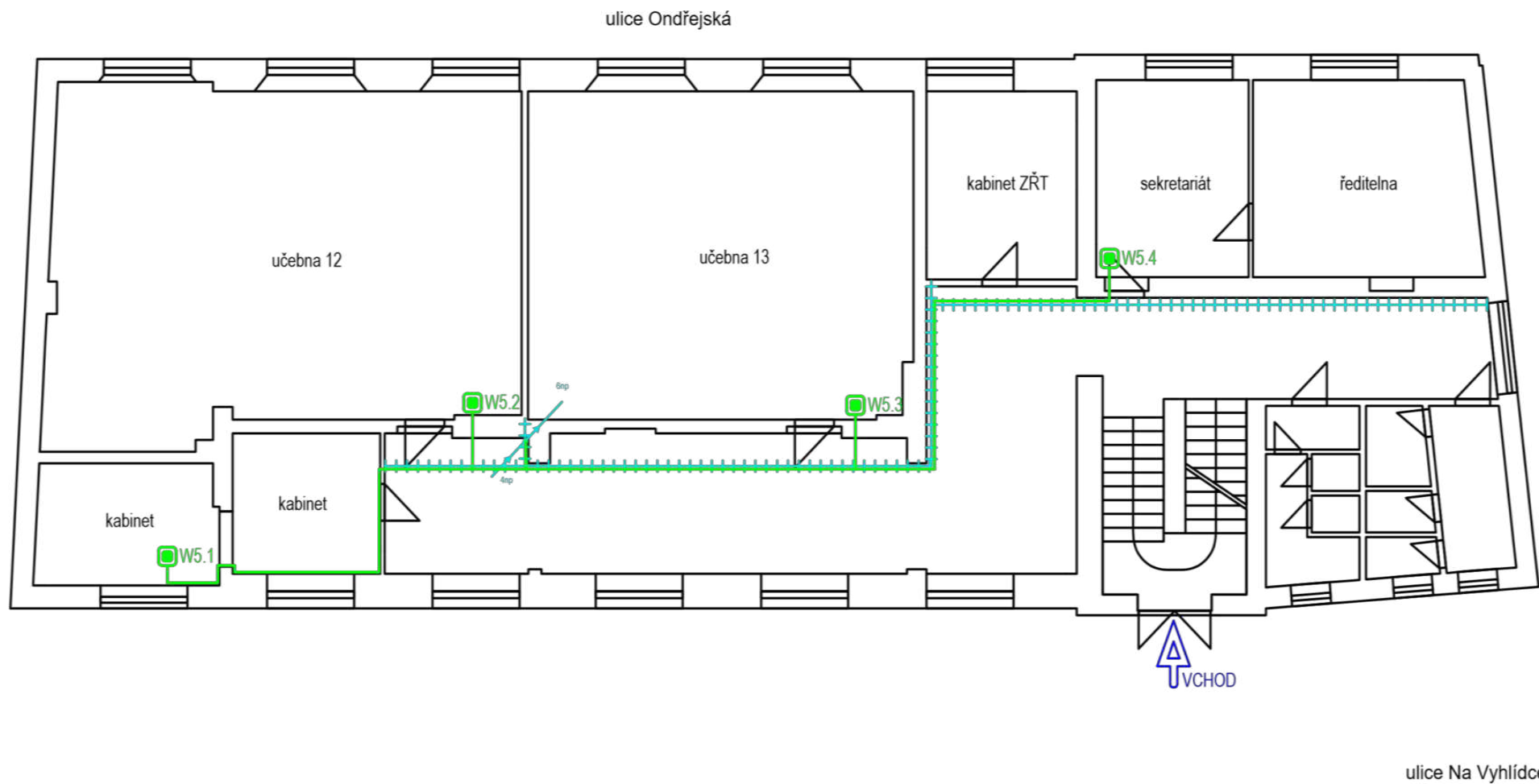


3. nadzemní podlaží

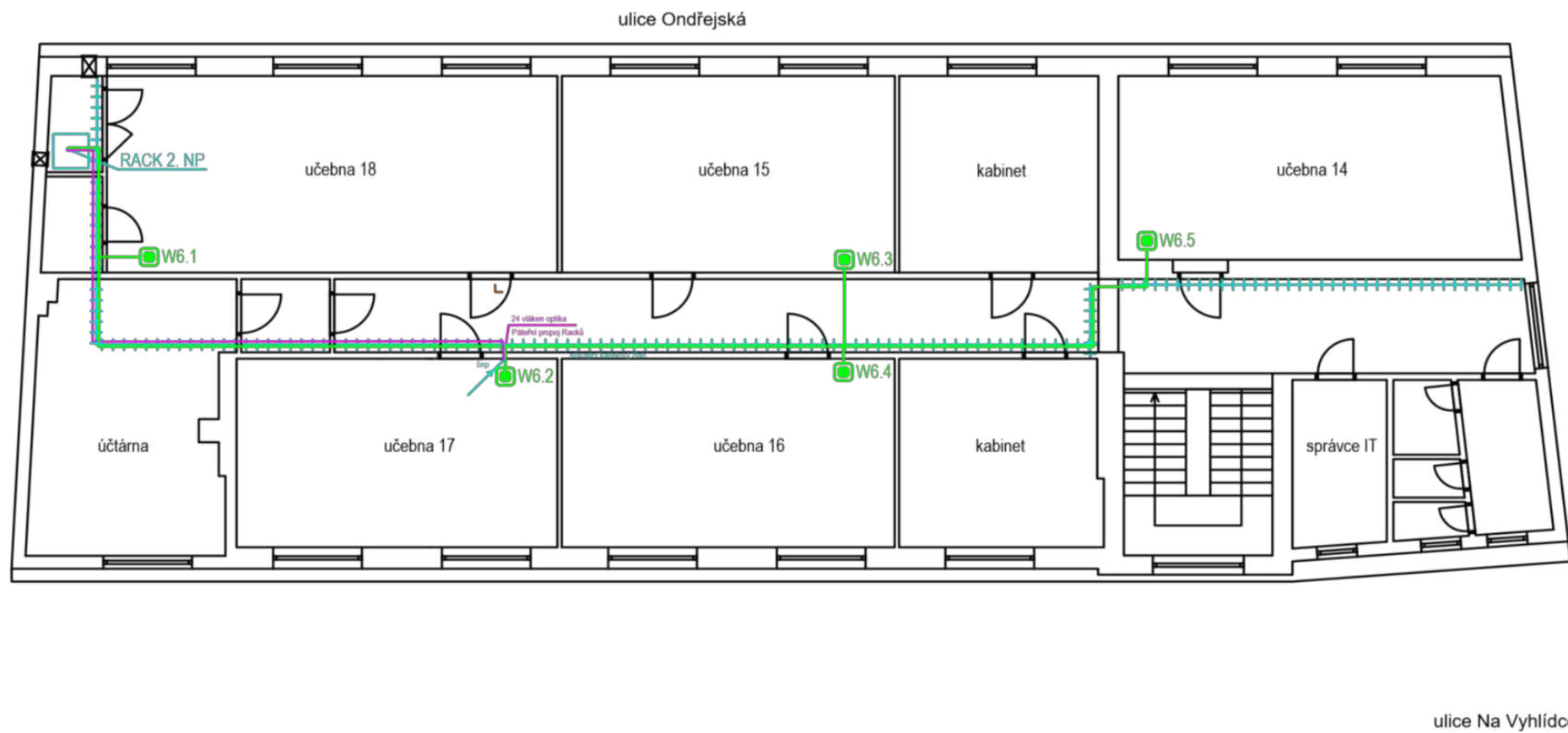


ulice Na Vyhlídce

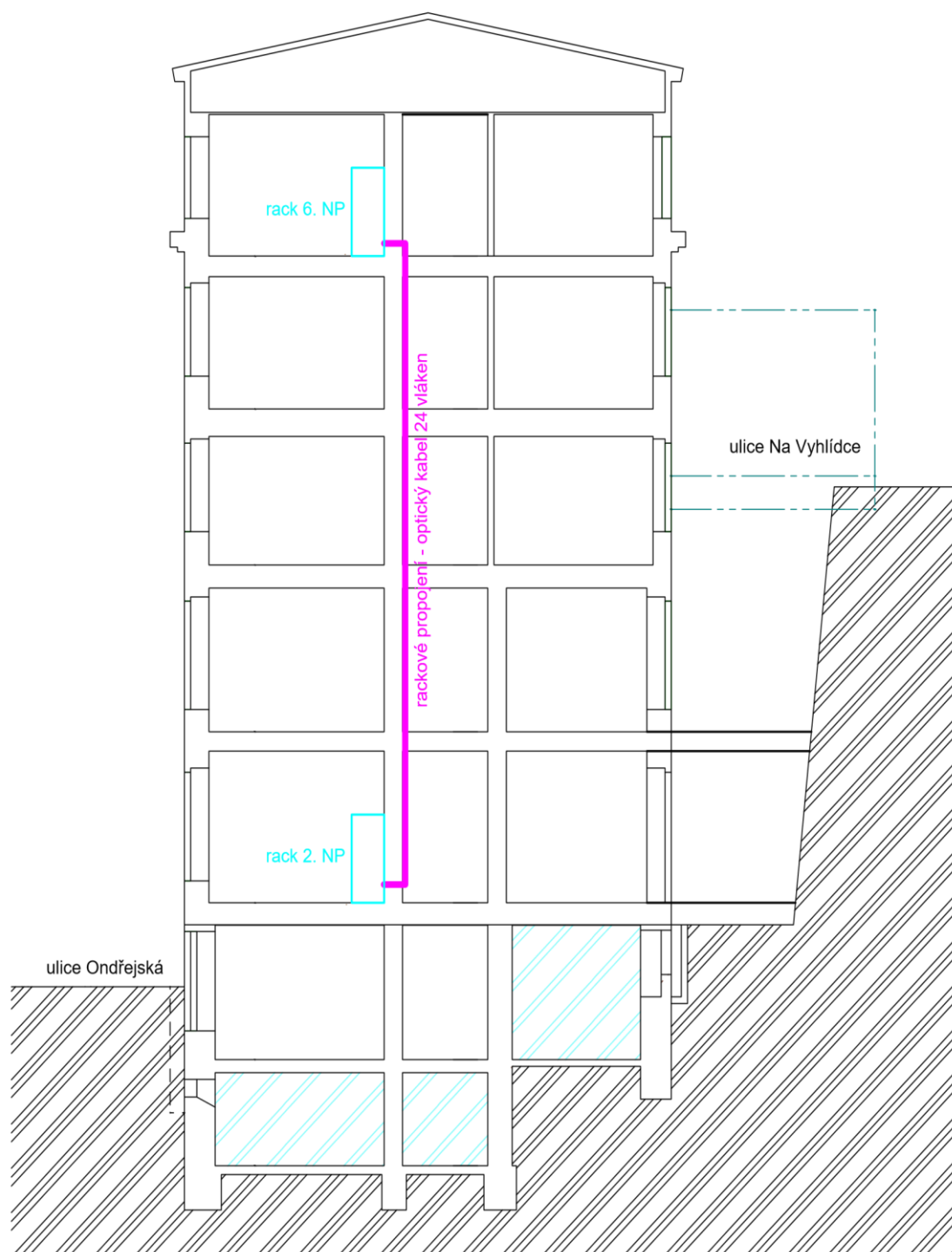
4. nadzemní podlaží



5. nadzemní podlaží



6. nadzemní podlaží



Řez budovou, rozmístění datových rovaděčů (racků)

Legenda:

metalické trasy a WiFi AP

optické trasy

stávající kabelové kanály, racky