

Technická dokumentace k veřejné zakázce „Konektivita budov Střední školy živnostenské Sokolov, p.o.“

OBSAH DOKUMENTACE

POPIS VÝCHOZÍHO STAVU.....	2
POPIS CÍLOVÉHO STAVU A SPECIFIKACE PŘEDMĚTU PLNĚNÍ.....	3
ZÁKLADNÍ POŽADAVKY NA TECHNICKÉ ŘEŠENÍ.....	3
SPECIFICKÉ POŽADAVKY NA TECHNICKÉ ŘEŠENÍ.....	3
<i>K1 – Virtualizační platforma</i>	<i>3</i>
<i>K2 – Zabezpečení LAN a Wi-Fi</i>	<i>4</i>
<i>K3 – Centrální logování a Správa identit</i>	<i>5</i>
<i>K4 – Systém pro evidenci a správu majetku.....</i>	<i>6</i>
<i>K5 – Kabelové rozvody LAN.....</i>	<i>6</i>
<i>K6 – Mobilní učebna.....</i>	<i>6</i>
IMPLEMENTAČNÍ SLUŽBY	6
ŠKOLENÍ.....	8
POPIS POVINNÝCH PARAMETRŮ DODÁVANÉHO ŘEŠENÍ	8
ZÁRUKY A SERVISNÍ PODMÍNKY	20
POŽADAVKY NA ZÁRUKY A SERVISNÍ PODMÍNKY	20
KABELOVÉ ROZVODY A DATOVÉ ROZVADĚČE	20

POPIS VÝCHOZÍHO STAVU

1. Střední škola živnostenská Sokolov, příspěvková organizace využívá pro svůj provoz 5 objektů. Jedná se hlavní budovu (sídlo školy) na adrese Žákovská 716 a objekty na adresách Nábřeží Petra Bezruče 2291, Karla Havlíčka Borovského 1267 a Heyrovského 1626 v Sokolově a budovu Školní 764 v Kynšperku nad Ohří. Školu navštěvuje přibližně 630 žáků.
2. Realizace projektu bude probíhat ve všech objektech školy.
 - a. Lokální sítě všech objektů jsou propojeny do jedné sítě:
 - b. bezdrátovými spoji v pásmech 24 a 60 GHz s centrálním bodem v budově Nábřeží Petra Bezruče 2291 na území města Sokolov
3. virtuální privátní sítě (VPN) realizovanou dodavatelem internetového připojení pro objekt v Kynšperku nad Ohří
4. Reálná přenosová kapacita spojů je až 1 Gbps u bezdrátových spojů a 100 Mbps u VPN
5. Současný stav ICT školy neodpovídá Standardu konektivity škol (dále jen Standard konektivity) ani současným nárokům na výkon, bezpečnost a centralizovanou správu počítačové sítě. Počítačová síť byla budována postupně, stáří a technické úroveň používaných prvků se liší. Převážně jde o prvky technicky i morálně zastaralé a výrobci nepodporované (nebo jen velmi omezeně). Chybí užší provázanost jednotlivých částí. Chybějící systém správy identit neumožňuje udržovat individuální elektronické identity pro všechny uživatele sítě (žáky i učitele) a následně automaticky uplatňovat politiky 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.
6. Kabelové rozvody v budovách školy jsou provedeny kabely různých kategorií (Cat3-Cat5). Kabeláž není plně strukturovaná a nevyhovuje jednotnému standardu. Pokrytí budov metalickými rozvody je nedostatečné a neumožňuje připojovat do sítě další zařízení (koncová zařízení, IoT a bezpečnostní prvky (kamery, rozhlas apod.)) a síť rozvíjet např. doplňováním Wi-Fi přístupových bodů. Nedostatek přípojných míst je řešen „rozbočováním“ sítě malými prepínači bez managementu, jejichž použití dále komplikuje správu celé sítě a snižuje její robustnost, stabilitu a bezpečnost. Kabeláž je uložena převážně ve vkladacích lištách. Kabelové rozvody pro kamerové, přístupové a obdobné systémy jsou vybudovány jako samostatné, oddělené od počítačových rozvodů. To znemožňuje konsolidaci sítě a její efektivní sdílení a řízení.
7. Propojení stanic i serverů je zajištěno převážně prepínači 100 Mb/s (částečně i 1 Gb/s) bez možnosti pokročilé správy. Aktivní prvky jsou umístěné převážně v datových rozvaděcích a nejsou dostatečně zabezpečeny proti neoprávněné manipulaci. Škola nevyužívá segmentaci pomocí VLAN, a to se negativně projevuje na její propustnosti a spolehlivosti. Aktivní prvky nesplňují požadavky na zabezpečení přístupu do LAN pomocí IEEE 802.1X.
8. Internetové připojení v současnosti zajišťují společnosti RETE internet, s.r.o. prostřednictvím spoje o rychlosti 100/100 Mbps. Rychlost připojení tak nesplňuje minimální požadavky Standardu konektivity škol 1– cca 150-160 Mbps (630 studentů x 0,25 Mbps nebo 300 počítačů x 0,5 Mbps). Připojení je poskytováno v budově Nábřeží Petra Bezruče 2291
9. Škola má přiděleny veřejnou IP adresy IPv4 a nemá IPv6. Škola nemá v současné době validující DNSSEC resolver na straně školy, neprovádí pokročilý monitoring provozu. Škola využívá internetovou doménu - živnostenska-sokolov.cz
10. Škola provozuje spojení Wi-Fi s omezeným pokrytím a nedostatečnou kapacitou pro připojení většího počtu klientských zařízení. Přístup k síti je řízen systémem voucherů vázaných na jméno uživatele a MAC adresu zařízení. chráněna mechanismem WPA-PSK (sdílené heslo). Wi-Fi je k dispozici zaměstnancům, studentům i hostům a partnerům. Prvky plně nepodporují aktuální bezpečnostní standardy (WPA3 apod.) ani pokročilé funkce optimalizace rádiového provozu a obsluhy připojených klientů. Není využíváno řízení přístupu klientů založené na standardu IEEE 802.1X
11. Zabezpečení přístupu k internetu využívá NG (next generation) firewall s rozšířenou sadou bezpečnostních funkcí IDS/IPS, URL filtrace, antivirové kontroly, aplikační kontroly, inspekce SSL provozu. Firewall nemá dostatečný výkon pro inspekci šifrovaného (SSL/HTTPS) provozu, který je v současné době převažující. Podpora výrobce stávajícího firewallu bude ukončena v srpnu 2026.
12. Škola provozuje 1 fyzický server virtualizovaný technologií VMware ESXi free. Hardware serveru již není výrobcem podporován a kapacitně i výkonově nepostačuje současným potřebám. Na serverech jsou využívány operační systémy Windows Server 2019 a Linux a provozovány webové aplikace, ekonomický systém, nástroje pro správu IT systémů a zálohování.

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

13. Zálohování dat a systémů je řízeno komunitní verze software Veeam Backup & Recovery. Funkce systému jsou omezeny ze strany bezplatné verze používaného hypervizoru. Zálohy jsou ukládány na externí diskové úložiště. Zálohy nejsou chráněny proti poškození či kompromitaci cíleným útokem.
14. Škola provozuje cca 300 koncových počítačů pro učitele a studenty. Na počítačích jsou používány operační systémy Windows 10 a vyšší s podporou domény Active Directory. Správa životního cyklu operačních systémů a aplikačního vybavení se provádí převážně manuálně s částečnou podporu cloudového systému Microsoft 365 (např. správa antiviru).
15. Pro ověřování uživatelů na počítačích je využívána cloudová adresářová služba Azure Active Directory. Není implementována a využívána lokální adresářová služba
16. Škola využívá cloudové služby Microsoft 365 A3 pro studenty i zaměstnance.
17. Pro zajištění potřebných aplikačních licencí produktů Microsoft škola využívá multilicenční program.
18. Škola využívá a prostřednictvím internetu vzdáleně zpřístupňuje ze své sítě webové aplikace Moodle, školní web. Školní web je dostupný prostřednictvím IPv4 šifrovaným protokolem https zabezpečeným certifikátem vydaným veřejnou certifikační autoritou. Výukový systém Moodle je dostupný pouze nešifrovaným protokolem http.
19. Školským informačním systémem je cloudový systém Škola OnLine provozovaný lokálně.

POPIS CÍLOVÉHO STAVU A SPECIFIKACE PŘEDMĚTU PLNĚNÍ

ZÁKLADNÍ POŽADAVKY NA TECHNICKÉ ŘEŠENÍ

1. Cílem projektu je zvýšení bezpečnosti a související modernizace IT infrastruktury, aby implementací projektu 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	Systém pro evidenci a správu majetku	1
K5	Kabelové rozvody LAN	1
K6	Mobilní učebna	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. 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.
4. 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.
5. 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.
6. 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.

SPECIFICKÉ POŽADAVKY NA TECHNICKÉ ŘEŠENÍ

K1 – Virtualizační platforma

1. Serverové technologie a hlavní síťové prvky budou umístěny v datovém rozvaděči v klimatizované místnosti.
2. Pro provoz veškerých pořízených systémů a aplikací bude pořízen nový virtualizační server vybavený rychlým a kapacitním (Tier 0 a Tier 1) interním úložištěm. Hardware serveru bude virtualizován a na serveru bude možno provozovat několik virtuálních serverů. Server bude připojen do sítě redundantní síťovou linkou o rychlosti min 10

Gb. Pořízený server musí být výrobcem určen pro provoz v běžném, neklimatizovaném prostředí do teploty 35 stupňů Celsia z důvodu odolnosti při výpadku klimatizace.

3. Pro zálohování bude v rámci projektu pořízeno síťové uložiště 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 umožní zálohovat i důležité osobní počítače.
4. Provozní zabezpečení bude tvořeno souborem non-IT technologií, které zajistí optimální podmínky pro spolehlivý chod technologií – především serveru:
 - a. Záložní zdroje napájení UPS zajistí chod serverů při výpadku napájení
 - b. Uzamykatelný rack zajistí bezpečné uložení serverů, správné větrání a zamezí neoprávněné manipulaci se serverem
5. Pro zajištění bezpečnosti a možnosti řízení provozu v síti a zajištění prokazatelného monitoringu, logování a auditu interního i externího síťového provozu bude aktualizována a rozšířena centrální databáze identit na bázi adresářové služby Active Directory. Adresářová služba umožní ukládání a přehlednou správu identit (účtů včetně metadat) učitelů, žáků i externích subjektů, ale i technických prostředků – serverů, tiskáren, pracovních stanic apod. Adresářová služba bude poskytovat službu LDAP a umožní snadné napojení autentizačních mechanismů a protokolů – radius, agenta 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.
6. Součástí platformy budou virtuální terminálový server pro bezpečný vzdálený přístup k provozním aplikacím prostřednictvím veřejných sítí (např. internetu) s využitím hardwarových nebo softwarových tenkých klientů.

K2 – Zabezpečení LAN a Wi-Fi

1. V rámci komodity budou do nově dodaných datových rozvaděčů dodány a osazeny nové aktivní prvky (firewally a přepínače), které budou doplněny zdroji záložního napájení (UPS). Pro bezdrátovou komunikaci Wi-Fi (a IOT) budou nasazeny moderní přístupové body (AP – access point) standardu Wi-Fi 6.
2. Všechny rozvaděče budou osazeny záložním napájecím zdrojem UPS.
3. Bude implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby s využitím technologie 802.1X.
4. 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.
5. Řízení provozu v LAN bude realizováno vytvořením VLAN (802.1Q), segmentací sítě s routováním (směrováním) provozu mezi VLAN na úrovni firewallu s nastavitelnými ACL. Pro řízení provozu na úrovni kvality služeb bude k dispozici technologie QoS (Quality of Services). Pro zajištění vysoké dostupnosti služeb budou klíčové aktivní prvky propojeny duálními trasami s automatickým rozkládáním zátěže a převzetím služeb v případě výpadku jedné trasy.
6. Architektura Wi-Fi bude založena na řešení s centrální správou prováděnou centrálním 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.
7. Umístění pořízených AP bude provedeno na základě provedené analýzy pokrytí signálem pro zajištění konzistentní Wi-Fi služby v pokrytých prostorách. Provedení analýzy bude součástí projektu.
8. 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.

9. Ověřování přístupu do Wi-Fi sítě bude realizováno na stejném principu jako LAN (tj. protokol 802.1X + radius). Wi-Fi 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 Wi-Fi), 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.
10. 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 uživatelské identity (centrální). Správcem systému EDU je společnost Cesnet. V rámci projektu bude realizováno připojení do systému EDUROAM a bude nakonfigurováno připojení Wi-Fi 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.
11. Pro zabezpečení veřejně publikovaných služeb a webových management nástrojů bude implementovány certifikáty vystavené veřejnou certifikační autoritou.

K3 – Centrální logování a Správa identit

1. Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací – může 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).
2. Veškeré dále požadované informace si bude systém automaticky získávat, vyčítat z monitorovaných systémů a současně bude umožňovat příjem protokolů určených pro přenos logovacích, provozních informací, alertů a událostí. Systém bude přijímat informace standardními protokoly ze síťových a dalších aktivních zařízení a Windows server systémů.
3. Mandatorní informace, která bude v systému vždy obsažena a uchována, je vazba IP-uživatel-čas. Tuto informaci bude systém čerpat ze security event-logu adresářové služby, dále z informací o probíhajících komunikacích prostřednictvím firewallu a dalších přístupových a autentifikačních systémů (např. radius logy). Dále budou získávány informace o překladu zdrojových, vnitřních IP adres na externím výstupním rozhraní firewallu, kde bude prováděn NAT. Bude se tedy jednat o informace obsažené v NAT tabulce. Spolu s tím musí být po stanovenou dobu možné zpětně dohledat i vnější provoz k vnitřnímu zařízení. Další funkcionalitou bude plnohodnotná práce se síťovými toky, jejich zpracování a archivace. Nástroje systému budou umožňovat i analytickou práci s přijímanými toky, a to i zpětně.
4. Kombinací požadavků Zákona o elektronických komunikacích č. 127/2005 Sb., spolu s požadavky Standardu konektivity škol a praktického pohledu na možné časové prodloužení 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.
5. V rámci komodity bude dále implementován systém pro správu identit (IDM – Identity management, nebo dále též systém). Systém bude čerpat údaje o uživateli (identitě) se školského informačního systému Bakaláři 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 úprav systému.
6. 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.
7. Součástí systému pro správu identit bude detailní logování prováděných změn pro možnost zjištění uživatelských oprávnění v libovolném času v minulosti (od nasazení systému).
8. 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 chybivosti 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.
9. 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.

K4 – Systém pro evidenci a správu majetku

1. Bude pořízen systém pro evidenci a správu prostředků (Asset management). Systém umožní evidenci jakéhokoli majetku. Je požadováno, aby systém dokázal automaticky (bezagentově) detekovat hardwarové konfigurace a softwarové vybavení počítačů v síti a umožnil provádět softwarový audit.
2. Správa prostředků bude umožňovat veškeré obvyklé operace s majetkem (pořízení, zavedení, převod, opravy, údržba, vyřazení apod.) včetně tisku příslušných předávacích protokolů a automatického upozorňování na opakované události (revize, údržba, kalibrace apod.). Pro správu IT majetku bude systém obsahovat obvyklé funkce pro podporu softwarového auditu (přehled, přidělování, odebírání licencí) v rozsahu akceptovaném hlavními výrobci software – např. Microsoft, Adobe, Autodesk.

K5 – Kabelové rozvody LAN

1. V rámci komodity bude vybudován strukturovaný kabelový systém vhodně využívající vyhovující části stávajících rozvodů. Systém zajistí spolehlivou komunikaci centrálních (serverových) technologií, napojení na stávající rozvody a dále napojení dodaných přístupových bodů Wi-Fi.
2. Centrálně bude umístěn hlavní datový rozvaděč pro uložení serverových a bezpečnostních technologií. Preferováno je umístění rozvaděčů mimo veřejné prostory a učebny (nebo alespoň mimo běžný dosah), aby byla minimalizována možnost přístupu neoprávněných osob.
3. Metalické kabelové rozvody budou provedeny metalickými kabely CAT 6. Optické trasy budou vedeny optickým kabelem se single-modovými vlákny a trasy budou obsahovat volná vlákna pro další rozšiřování či náhradu poškozených vláken.

K6 – Mobilní učebna

1. V rámci komodity bude dodáno vybavení mobilní učebny, která bude plně integrovaná do sítě LAN a WAN.

IMPLEMENTAČNÍ SLUŽBY

1. V rámci implementace předmětu plnění dodavatel realizuje pro všechny nabízené komodity K1 až K5 – následující služby, které 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 practices) 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:
 - Adresářová služba – správa uživatelů a skupin, zařazení počítače do domény
 - Zálohování – kontrola činnosti, obnova souborů
 - Hypervizor – ovládání virtuálních serverů, změna jejich konfigurace
 - Logovací systém – vyhledávání činnosti uživatelů a systémů, běžná správa a kontrola funkce
 - LAN a Wi-Fi – připojení zařízení vč. podrobných **uživatelských** postupů pro Wi-Fi připojení mobilních zařízení (tablety, chytré telefony, notebooky) s operačními systémy Windows 10 a vyšší, Android, iOS a macOS.
 - Firewall – blokování stránek, dohledání činnosti uživatele, práce s kategoriemi stránek, zablokování přístupu pro uživatele skupinu
 - 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 Školení
 - 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 - Návrh a kompletní implementace serverové virtualizační platformy včetně systému terminálových služeb s publikační bránou do veřejných sítí - Implementace pořízených technologií - Analýza dat a stávajících sdílených systémů a jejich migrace na novou platformu - Návrh vhodné struktury adresářové služby, její vytvoření a naplnění identitami - Návrh a realizace zálohovacího řešení včetně nastavení zálohovacích plánů. - Implementace automatické odstávky serveru v případě výpadku dodávky elektrické energie - Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy a testy vysoké dostupnosti, je-li architektura tak navržena.
K2: Zabezpečení LAN a Wi-Fi - Analýza stávajícího síťového prostředí a návrh nového architektury LAN i Wi-Fi - Implementace pořízených technologií - Provedení segmentace LAN – VLAN, adresování, směrování - Zavedení IPv6 pro přístup k internetovým zdrojům publikovaným na IPv6 adresách - 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 zivnostenska-sokolov.cz, DNS, e-mail, web školy, popř. publikace školského systému pro rodiče - Zabezpečení komunikace publikovaných služeb školy pomocí certifikátu. - Zavedení DNSSEC pro interní DNS služby i zabezpečení domény zivnostenska-sokolov.cz - Návrh a implementace 802.1X pro kabelovou LAN i Wi-Fi včetně uživatelské dokumentace pro konfigurace obvyklých zařízení a jejich systémů – PC, notebooky, chytré telefony, tablety, tiskárny – Windows, Linux, MacOS, Android, IOS, embedded systémy periferií - Návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) pro školu - Vybudování VPN pro vzdálený přístup uživatelů LAN na bázi webového portálu - Respektování min. 3 různých skupin uživatelů (učitelé, studenti, hosté) v návrzích a implementaci bezpečnostních a ostatních politik - Implementace portálu pro registraci a řízení přístupů hostů – tzv. captive portál - Implementace připojení k EDUROAM a zpřístupnění v prostorech školy včetně podpory jednání a řízení změn s provozovatelem (CESNET) a organizačních opatření – zpracování textů pro web školy, zapracování do Zásad využívání ICT - Zajištění ostatních nezbytných činností pro naplnění Standardu konektivity
K3: Centrální logování a Správa identit <u>CENTRÁLNÍ LOGOVÁNÍ</u> - 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. - 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 b. Další požadované služby • kompletní implementace systémů podle předimplementační analýzy a prováděcí dokumentace • metodické a odborné vedení pracovníků škol při jednání o poskytnutí potřebných rozhraní na straně školského informačního systému. 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: Systém pro evidenci a správu majetku
a. Analýza životního cyklu evidovaného majetku b. Návrh konfigurační databáze pro zavedení do systému c. Návrh způsobu automatické inventarizace koncových zařízení (počítačů a notebooků) d. Návrh vhodného způsobu iniciačního zavedení evidovaného majetku (naplnění databáze) e. Implementace systému dle provedených návrhů a doporučení výrobce f. Návrh a provedení akceptačních testů
K5: Kabelové rozvody LAN
a. Dodávka a kompletní oživení kabelového systému včetně certifikačního měření prokazujícího splnění standardů Cat6 metalických rozvodů a obvyklých kvalitativních parametrů optických tras a požadovaných parametrů systému poskytovaných po dobu záruky
K6: Mobilní učebna
b. Dodávka a kompletní instalace mobilní učebny, včetně zaškolení obsluhy

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 uchazeč 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 v písemné formě vhodné jako příloha k Závěrečné zprávě o realizaci projektu. **Účastník již v nabídce předloží čestné prohlášení potvrzující, že výše uvedené požadavky jím navržené technické řešení splňuje, a to v rámci přílohy č. 6 zadávací dokumentace.**
6. 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:
 - 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.

POPIS POVINNÝCH PARAMETRŮ DODÁVANÉHO ŘEŠENÍ

Komodita K1 – Virtualizační platforma		
Část	Parametr	Popis povinného parametru

Server s příslušenstvím 1x	Provedení	rackové provedení max. 2U včetně výsuvných kolejnic a montážního materiálu do racku (datového rozvaděče).
	CPU	1x procesor, maximálně 16 jader Procesorový výkon dle https://spec.org/ minimálně: SPECrate®2017_int_base 176 bodů SPECrate®2017_fp_base 228 bodů
	RAM	512 GB, DDR5, min. 4800 MT/s, výkonově optimalizovaná konfigurace
	Úložiště pro hypervizor	Min. 2x M.2 SSD 480 GB, RAID1, nezabírá pozice HDD, podpora výměny disků za provozu
	Úložiště	in. 4x 3.6 TB SSD 3 DWPD (mixed use), 5x 8TB 7200 ot/min, podporu výměny za provozu (hot-swap)
	Rozšiřitelnost	Min. 2 volné pozice HDD pro rozšíření kapacity, s možností osazení disků SATA/SAS. Všechny pozice aktivní, připojené k řadič
	RAID hardware	SAS/SATA/NVMe řadič se zálohovanou vyrovnávací pamětí min. 8 GB. Podpora RAID 10,50 a 60 režimu.
	LAN	Porty min. 2x 1GbE, 2x 10/25 Gb SFP28 Všechny NIC s podporou virtualizace – VMware NetQueue, Microsoft VMQ. 1x 1GbE – samostatný port pro vzdálený management
	USB	min. 2x USB porty, z toho min. 1x na čelním panelu s podporou bootování a 1x USB 3
	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 Monitorování a řízení spotřeby. HTML5 rozhraní Stavové informace na čelním panelu s výraznou indikací nestandardních a chybových provozních stavů či parametrů (min. napájení, teplota, vada HDD. Aktivní indikace standardního provozního stavu. V případě závady zobrazuje její popis v textové formě.
	Provozní podmínky	Určen a výrobcem podporován pro provoz v běžném neklimatizovaném prostředí min. do 35 stupňů Celsia
	Napájení	2x napájecí zdroj s výkonem min. 1000 W, redundance, min. Titanium specifikace dle 80 PLUS https://cs.wikipedia.org/wiki/80_Plus
	Záruka	60 měsíců poskytovaná výrobcem, oprava následující pracovní den od nahlášení v místě instalace, technická podpora výrobce v českém jazyce. Dostupnost ovladačů a dokumentace na webu výrobce dle výrobního/sériového čísla serveru.
Licence operačních systémů serverů a klientské licence	Serverové operační systémy	2 ks licencí 64-bitového 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	300 ks klientských licencí vázaných na zařízení k nabízeným operačním systémům
Záložní zdroj UPS pro server 1x	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
	Účinnost	lepší než 0,98
	Stabilizace	výstupní napětí – odchylka max. ±5 % od jmenovité hodnoty
	Kapacita	doba 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
	Komunikační porty a rozhraní	RS-232, USB

	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 shutdown 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
Licence zálohovacího software	Licence	trvalá licence zálohovacího software pro nabízený server bez omezení počtu zálohovaných virtuálních serverů a objemu dat.
	Efektivita ukládání dat	integrován 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
	Úložiště 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)
	Cloud	podpora zálohování prostředí Microsoft 365 (soubory, e-mailů atd.)
	Záruka	60 měsíců včetně nároku na opravné a nové verze
Sít'ové úložiště NAS 1 ks	Provedení	samostatně stojící provedení s možností uložení do racku do racku.
	Výkon	64 bit CPU, min. 4 jádra
	HDD	Min. 8 pozic pro HDD, rozšiřitelné min na 16 HDD
	Rozšiřitelnost	Podpora připojení externích disků přes USB 3.0 (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. 2 x 1 GbE porty s podporou agregace linek a redundance
	Výkon	Rychlost zápisu min. 1 200 MB/sec při RAID5 a SMB/CIFS v nabízené konfiguraci
	Kompatibilita	Plná podpora Microsoft Hyper-V a Windows Active Directory a ACL.
	Komunikace LAN	Sít'ové protokoly CIFS, WebDAV, iSCSI, SSH, SNMP, http/s
	UPS	Podpora korektního vypnutí signálem z UPS přes LAN při výpadku napájení
	RAM	min. 8 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 a aktualizací firmware

Komodita K2 – Zabezpečení LAN a Wifi

Část	Parametr	Popis povinného parametru
------	----------	---------------------------

Firewall 2x	Porty	min 10x 1GbE (min. 2x WAN) a 2x 1 Gb SFP (mohou být sdílené), USB pro ext. modem
	NGFW	Min. základní funkce Next-generation firewall – vizte 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. 1,4 milionu
	Propustnost SSL VPN	min. 900 Mbps, při licenčním nebo technickém omezení počtu klientů požadujeme min. 25 klientů
	Propustnost SSL inspekce	min. 700 Mbps
	Propustnost firewallu	min. 10 Gbps pro pakety 512 bytů a větší
	Propustnost NGFW	min. 800 Mbps
	Propustnost IPS	min. 1000 Mbps
	Propustnost detekce škodlivého kódu	min. 500 Mbps
	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	integrován antivirus, podpora protokolu ICAP pro offload AV detekce, možnost detekce tzv. Grayware (rootkit, malware, spyware, keylogger, atd.)
	Kategorizace a blokáce provozu	založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorií na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne
	Antispam	antispamová a antivirová inspekce elektronické pošty
	Sandbox	integrován 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	integrována podpora SD WAN - min. rozkládání zátěže a vysoká dostupnost více internetových přípojek
	Sledování toků	export síťových toků (Netflow nebo ekvivalent)
	Standardní funkce	NAT, statické a dynamické routování, 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)
Centrální přepínač školy 2x	Základní parametry	L2/L3 přepínač v rackovém provedení max. 1U, neblokovaná architektura (přepínací kapacita min. 880 Gbps)
	Porty	24x 10 Gb SFP + 2x 100 Gb QSFP28 (kompatibilní s 40Gb QSFP+ a podporou rozdělení každého na 4x 10/25Gb porty)
	Agregace portů	podpora LACP, min. 20 portů v agregační skupině, bez omezení počtu skupin
	Směrování	hardwarové statické routování včetně VLAN, dynamické směrování (min. RIP, OSPF, BGP), směrování založené na politikách, min. 8000 routovacích záznamů pro IPv4 i IPv6
	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), podpora VXLAN, min. 4000 VLAN
	Ověřování uživatelů a zařízení	Podpora 802.1X
	Dualstack	plný IPv4 a IPv6 dualstack včetně směrování a QoS
	MAC	podpora min. 60 000 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, odeslání náhradního zařízení max. následující pracovní den, včetně opravných verzí firmware
Přístupové přepínače 14x	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
	Specifické parametry	
	Počty, porty a propustnost, PoE výkon (budget)	8x přístupový přepínač – 48x 1 Gb RJ-45 PoE + 4x 10 Gb SFP+, 176 Gbps, PoE min. 730W 1x přístupový přepínač – 48x 1 Gb RJ-45 PoE + 4x 10 Gb SFP+, 176 Gbps, 4x přístupový přepínač – 24x 1 Gb RJ-45 PoE + 4x 10 Gb SFP+, 129 Gbps, PoE min. 370W 1x přístupový přepínač – 24x 1 Gb RJ-45 PoE + 4x 10 Gb SFP+, 129 Gbps,
Wi-Fi přístupové body 74 ks	Základní funkce	Přístupový bod (AP) standardu Wi-Fi 6 včetně montážního materiálu na strop
	Frekvence	min. 3 nezávislé rádiové moduly činnost v rádiovém pásmu 2,4 a 5 GHz současně, s podporou standardu OFDMA min. u 2 modulů
	Architektura	Homogenní Wi-Fi 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 (Wi-Fi sítí) na 2.4 i 5 GHz současně, podpora přiřazení každého SSID do samostatné VLAN
	Zatížení	min. 300 přiřazených (asociovaných) klientů na rádiový modul
	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 Wi-Fi 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 (Wi-Fi 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)
	Záruka	min. 60 měsíců poskytovaná výrobcem zařízením, včetně opravných verzí firmware
Licence síťových prvků (sada)	Licence	Licence pro využití veškerých požadovaných funkcionalit síťových prvků (firewall, přepínače, přístupové body), pokud nabízené řešení takové licence vyžaduje.
	Podpora a platnost	min. 60 měsíců poskytovaná výrobcem
Optické prvky	SFP moduly	56 ks modulů SFP+ 10 Gb, SM min. 1 km, včetně DMI diagnostiky pro nabízené přepínače, LC konektor 2x kabel 1xQFSP+ => 4xSFP+, 5 m pro nabízené přepínače a servery
	Patch kabely	28 ks optický kabel SM s konektory LC-SC, délka 1 m 28 ks optický kabel SM s konektory LC-SC, délka 2 m
	Záruka	min 36 měsíců
Záložní zdroje UPS pro LAN prvky 4x	Provedení	provedení do racku, max. 2U, včetně montážního materiálu
	Elektrické provedení	jmenovité napětí 230 V, jednofázová na vstupu i výstupu
	Výkon (VA/W)	1000 VA / 900 W
	Technologie	online, dvojitá konverze
	Účinnost	min 0,9
	Stabilizace	výstupní napětí – odchylka max. ±5 % od jmenovité hodnoty
	Kapacita	doba běhu na baterie min. 8 min při 50% zátěži
	Vstup	zásuvka IEC C14
	Výstupy	min. 3 zásuvky 230 V – standardní kulaté (podpora UNISCHUKO zástrček) nebo IEC-13
	Diagnostika	Vestavěný úplný systémový autotest, možnost automatického plánovaného provádění
	Bypass	automatický interní bypass
	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
	Rozměry	max. hloubka 320 mm (pro umístění do racku)
	Záruka	24 měsíců včetně baterií
1x Licence pro řízení přístupu do sítě IEEE 802.1X	Provedení	Software pokročilého řešení NAC (network access control) na bázi standardu IEEE 802.1X. Integrovaná podpora autentizace, autorizace a účtování (přístupů) uživatelů i koncových zařízení, integrovaný RADIUS server a databáze uživatelů a zařízení.
	Nastavení přístupů	Nastavení síťového přístupu uživatelů a zařízení podle politik min. pomocí přiřazení VLAN, ACL. Atributy pro definici politik min. IP, MAC, port, VLAN, QinQ VLAN, hostname (PC name), uživatelské jméno (z Active Directory), operační systém
	Autentizace	Zajištění IEEE 802.1X autentizace a autorizace pro bezdrátové sítě, Ethernet LAN sítě a VPN
	Základní autentizační metody	Min. PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace, certifikáty
	Identity	Vestavěná databáze identit pro autentizaci, podpora standardních identitních databází – Active Directory

	Kontextová autorizace	Autorizace zařízení a uživatelů na základě kontextových informací jako čas, typ připojení, osobní profil či členství ve skupině v Active Directory.
	Speciální zařízení	Podpora autentizace a řízení přístupů speciálních ("nepočítačových") zařízení např. tiskárny, technologické prvky, IoT.
	Licence	Licence pro min. 1000 konkurenčních koncových zařízení ověřovaných pomocí 802.1X bez omezení počtu uživatelů.
	Automatizace a integrace	REST-API rozhraní min. pro základní funkce AAA, hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně.
	Kompatibilita	Systém určený pro provoz v prostředí stávající serverové virtualizace
	Záruka	Záruka min. 60 měsíců, včetně podpory výrobce a nároku na opravné software včetně aktualizací.
1x Infrastruktura veřejných klíčů	Provedení	PKI (Public key infrastructure) pro správu a distribuci veřejných klíčů asymetrické kryptografie.
	Architektura	Interní certifikační autorita pro vydávání certifikátů na základě šablon a oprávnění pro uživatele i zařízení, veřejná dostupnost CRL (certificate revocation list)
	Integrace	S adresářovou službou Active Directory (oprávnění, ukládání veřejných klíčů) a nabízeného systému pro správu identit (evidence, platnost)
	Správa	Plně grafické prostředí pro správu i uživatelské operace s certifikáty, včetně odvolání certifikátu. Podpora prodloužení platnosti certifikátu uživatelem, upozornění na blížící se expiraci, řízení oprávnění k prodloužení.
	Schvalování	Ruční i automatické schvalování žádosti o certifikát nebo jeho prodloužení. Konfigurovatelné pro jednotlivé šablony.
	Zálohování, obnova	Obnova primárního klíče „ztraceného“ certifikátu
	Automatizace	Standardizované a dokumentované REST API nebo skriptovací nástroj pro automatizace životního cyklu certifikátů
	Licence	Bez omezení počtu vystavovaných certifikátů a jejich typů/šablon
	Záruka	60 měsíců včetně nároku na opravné verze

Komodita K3 – Centrální logování a Správa identit		
Část	Parametr	Popis povinného parametru
Licence pro sběr a správu logů (log Management) 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	integrováný 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	sodpora 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
	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.
	Alerty, notifikace	podpora vytváření alertů – překročení okamžitých či kumulovaných hodnot, zasílání upozornění
	Active Directory	integrace s Active Directory pro ověřování uživatelů, nastavení oprávnění min. administrator a operator

	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
Licence SW pro správu identit (identity management IdM) včetně Licence SW modulů/API pro integraci IdM 1x	Základní funkce	IDM (dále IDM nebo Systém) bude udržovat a spravovat identity a organizační strukturu organizace – třídy, učitelů, 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 systémů 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	integrovatelný 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 databázová 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 objektů 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).
	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 delegovanu.
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/správce IDM budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy změnil 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 běhy 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 odstávky a výběru synchronizované organizace bude součástí Portálu.
Zdrojový systém	IDM bude napojen na školský informační systém Bakaláři https://www.bakalari.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 - 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 – Systém pro evidenci a správu majetku		
Část	Parametr	Popis povinného parametru
Licence SW pro evidenci a správu majetku (Asset management)	Základní požadavky	systém pro správu a technickou provozní evidenci veškerého počítačového i ostatního majetku (aktiva). Systém bude určený technicky i licenčně pro podnikové nasazení s profesionální podporu výrobce
	Podpora procesů dle ITIL	systém musí pokrývat následující procesy dle doporučení ITIL: - Asset and Configuration Management - Software Asset Management
	Implementované procesy a funkce	z procesu Asset and Configuration Management budou implementovány min. následující funkce: - podpora správy konfigurační databáze, musí být uchovávána historie konfiguračních položek - podpora automatizace zjišťování informací o konfiguračních položkách hardware Z procesu Software Asset Management budou implementovány min. následující funkce: - řízení životního cyklu spojeného se softwarovými aktivy - automatické zjišťování informací o konfiguračních položkách software - podpora operativní práce IT správců spojená s řešením a udržením softwarové a licenční čistoty.
	Typy majetku	systém umožní evidovat a spravovat libovolný druh majetku, kromě IT zařízení např. vozidla, nemovitosti, vybavení tříd a kanceláří, pracovní prostředky a nástroje apod.
	Automatický sběr dat	systém umožní automatický neinvazivní (bezagentový) sběr údajů o hardware a software z počítačů
	Neznámý software	automatické odeslání vzorků nerozpoznaného software výrobcí k analýze a automatické stažení aktualizovaných signatur pro rozpoznávání.
	Mobilní zařízení	počítače umístěné mimo LAN zadavatele budou se systémem komunikovat zabezpečeným protokolem prostřednictvím internetu bez nutnosti použití VPN
	Vizualizace	grafické zobrazení evidovaného majetku a dalších hlavních struktur/objektů systému (např. organizační jednotky, skupiny uživatelů) v hierarchické struktuře. Struktura musí být volně upravitelná podle potřeb Zadavatele
	Řízení oprávnění	systém umožní nastavit oprávnění na úrovni vlastností objektů - např. zamezit zobrazení pořizovací ceny uživatelům
	Rozšiřitelnost	systém umožní přidávat do systému libovolné objekty a přidávat k těmto objektům libovolné vlastnosti.
	Dokumenty	v systému musí být možno ukládat libovolné elektronické dokumenty (pořizovací doklady, licenční certifikáty apod.) a tyto dokumenty propojit s konkrétním objektem nebo více objekty.
	Platnost dokumentů	dokumenty bude možno v systému zneplatnit (v systému zůstanou zachovány)
	Dědičnost	systém bude podporovat dědičnost vlastností objektů
	Protokoly	předpřipravené podpisové protokoly pro formální úkony při správě majetku (předání/převzetí/převod).
	Zabezpečení přístupu	zabezpečený přístup do aplikace včetně integrovaného přihlašování do uživatelského prostředí i u konzol, řízení oprávnění přístupu k informacím.
	Historie záznamů	systém musí umožnit automaticky evidovat změny provedené s jednotlivými objekty. Rozsah změn min. přesuny, instalace, předávací protokoly včetně informace kdo, kdy změnu provedl.
	Reporty	systém musí umožnit vytváření vlastních pohledů, filtrů a exportů min. do Microsoft Excel.
	Zaměstnanecký portál	umožňuje zaměstnancům kdykoli zobrazit aktuální stav svěřeného majetku prostřednictvím webového prohlížeče
	Intuitivní ovládání	snadná orientace v přehledech majetku, možnost přetahování položek myší, podpora kontextových menu pro rychlé úpravy a eliminaci chyb
	Lokalizace	rozhraní systému pro uživatele i správce bude plně lokalizováno do českého jazyka
	Vyhledávání	integrované vyhledávání a filtrování
	Automatické názvy	systém musí umožnit automatické pojmenovávání spravovaných zařízení, min. pomocí definice (přednastavení) číselné řady.
	Řízení změn konfigurace	systém musí umožnit evidenci konfigurace systémů a zařízení.
	Vzdálená správa	systém bude možno integrovat s nástroji pro vzdálenou správu počítačů - min. Vzdálená plocha Windows, VNC a Microsoft Management Console
	Elektronická inventura	integrovaná elektronická inventura – zaměstnanci explicitně potvrdí v prostředí portálu trvající existenci a používání svěřeného majetku. Hromadná kontrola inventur správci majetku.
	API	systém musí umožnit rozšíření pomocí otevřeného rozhraní API na bázi webových služeb.
	Import	systém musí umožnit import majetku min. ze souborů csv
	Správa uživatelů	systém bude integrován s Active Directory, bude přebírat uživatele včetně jejich vlastností a organizační hierarchie (nadřazený/podřazený)

	ITIL	nabízená hlavní verze systému musí být certifikována na shodu se standardy ITIL. Plnění požadavku bude prokázáno certifikátem přiloženým k nabídce
	Licence	licence musí umožnit spravovat 200 počítačů a min. 8 000 ostatních aktiv. Poskytnutá licence bude trvalá
	Podpora	60 měsíců včetně nároku na opravné verze a aktualizace signatur pro rozpoznání hw a sw

Komodita K5 – Kabelové rozvody LAN		
Část	Parametr	Popis povinného parametru
Kabelové rozvody vnitřní	Popis	Kabelové rozvody včetně příslušenství a souvisejících služeb dle podrobného výkazu výměr – Kapitola KABELOVÉ ROZVODY A DATOVÉ ROZVADĚČE
	Záruka	Kabelové rozvody 10 let, rozvaděče 24 měsíců

Komodita K6 – Mobilní učebna		
Část	Parametr	Popis povinného parametru
Interaktivní displej	Velikost obrazovky:	Interaktivní displej s úhlopříčkou min. 75" (190cm)
	Rozlišení LCD:	rozlišením obrazu 4K UHD
	Dotyková technologie	Dotyková technologie umožňuje odlišit dotyk prstem (pro ovládání) a popisovačem (pro psaní) a také odlišit popisovače (např. pro psaní různou barvou).
	PC	Součástí displeje musí být počítačový modul s minimálními parametry 4GB RAM a 32GB HDD
	Rozhraní:	Pro připojení má displej minimálně konektory HDMI a USB-C,
	Konektivita	bezdrátovou konektivitu Wifi (2,4 i 5GHz) a Bluetooth (min. verze 4.2)
	Rozšíření	slot pro integraci plnohodnotného učitelského PC.
	Příslušenství	včetně systémové AV kabeláže, VESA montáž
	Kabel HDMI a extender	Kabel HDMI, min. 4K*2K @ 60Hz, min. 10m. Včetně HDMI extenderu pro zesílení signálu podporující přenos na min. 30 m, podpora rozlišení min. 4K*2K @ 60Hz. Včetně HDMI kabelu 0,5 m, (M/M), min. rozlišení 4K*2K @ 60Hz.
	Repeater aktivní USB	USB repeater pro prodlužování USB kabelů, délka min. 5 m.
	Záruka	min. 24 měsíců
Pojízdný stojan	Parametry	Elektricky výškově nastavitelný mobilní stojan. Kolečka s brzdou. VESA montáž LCD
Konvertibilní NB 30x	Provedení	Konvertibilní notebook s odnímatelnou klávesnicí s úhlopříčkou min 10" a zároveň max 13"
	Displej	rozlišení min. 1920 x 1280, provedení IPS, dotykový
	CPU	výkon CPU dle https://www.cpubenchmark.net min. 3000 bodů, nízká spotřeba - TDP do 10W
	Video	výkon video/grafického procesoru dle https://www.videocardbenchmark.net min. 750 bodů
	RAM	min. 8 GB DDR3
	HDD	min. 120 GB SSD
	Bezdrátové připojení	Wi-Fi 802.11 ac, 2,4 + 5 GHz, podpora 802.11 n/ac/ax Bluetooth min. 4.2
	Porty	min. 1x USB - C
		min. 1x audio
	Kamera	min. 1 Mpix
	Hmotnost	max 1200g
	Reproduktory	integrované reproduktory
	Klávesnice	odnímatelná podsvícená klávesnice s touchpadem, českým rozložením kláves
	Napájení	kapacita baterie pro min. 8 hodin provozu, odpovídající napájecí adaptér
	Software	Operační systém Microsoft Windows v aktuální verzi s podporou domény Active Directory, 64 bitový, české rozhraní
	Záruka	Záruka min. 36 měsíců poskytovaná výrobcem

Box pro uložení a napájení tabletů	Provedení	Box pro bezpečné uložení a současného nabíjení všech nabízených tabletů. Musí umožnit uložení a nabíjení tabletů včetně připojených klávesnic
	Zabezpečení	Uzamykatelný, robustní provedení vhodné i pro převážení
	Nabíjení	Automatické a ruční řízení nabíjení
	Rozměry	Box musí mít takové rozměry, aby bylo možné jednoduše projít dveřmi
	Záruka	Záruka min. 12 měsíců
	Parametry	Náhlavní souprava, propojení USB, zabudovaný mikrofon
Náhlavní souprava 31x	Parametry	Náhlavní souprava, propojení USB, zabudovaný mikrofon
Notebook pro učitele	Provedení	Notebook s úhlopříčkou min. 14" a zároveň max. 15,4"
	Displej	rozlišení min. 2496x1664, provedení IPS, dotykový
	CPU	výkon CPU dle https://www.cpubenchmark.net min. 8000 bodů,
	Video	výkon video/grafického procesoru dle https://www.videocardbenchmark.net min. 750 bodů
	RAM	min. 8 GB DDR3
	HDD	min. 500 GB SSD
	Bezdrátové připojení	Wi-Fi 802.11 ac, 2.4 + 5 GHz, podpora 802.11 n/ac/ax
	Bezdrátové připojení Porty	Bluetooth min. 4.2 min. 1x USB - C
	Kamera	min. 1 Mpix
	Hmotnost	max 1700g
	Reproduktory	integrované reproduktory
	Klávesnice	klávesnice s touchpadem, českým rozložením kláves
	Napájení	kapacita baterie pro min. 8 hodin provozu, odpovídající napájecí adaptér
	Software	Operační systém Microsoft Windows v aktuální verzi s podporou domény Active Directory, 64 bitový, české rozhraní
	Záruka	Záruka min. 36 měsíců poskytovaná výrobcem
Výukový SW anglického jazyka	Bezdrátová komunikace	SW optimalizovaný bezdrátový provoz
	Forma výuky	Možnost individualizovat výuku
	Záznam	Možnost monitorovat a nahrávat konverzaci studentů
	Řízení výuky	Podpora stálé kontroly výuky, centrálního blokování internetu a dálkového ovládání aplikací
	Úkoly	Musí umožňovat zadávat a sbírat domácí úlohy
	Testy	Podpora distribuce úkolů a testů na jednotlivé PC a jejich stahování zpět (odevzdání)
	Výukové materiály	Snadný převod stávajících učebních materiálů do formátu mp3 či tvorbu nových materiálů za chodu
	Interaktivita	Podpora spolupráce se studenty pomocí interaktivní plochy "bílá tabule" a nástroje "zvýrazňovací pero"
	Licence	Licence pro minimálně 30 zařízení

ZÁRUKY A SERVISNÍ PODMÍNKY

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.
2. 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 (vizte Příloha č. 2 Zadávací dokumentace) do samostatných řádků označených vždy názvem položky a upřesněním prodloužené záruky. Obdobně bude vyčíslen záruční servis u komponent, u kterých je požadován. Tyto náklady nebudou hrazeny z dotace, proto je nutné vyčíslit je zvlášť.
3. Zadavatel v rámci této technické specifikace požaduje specifické služby, které se odvíjejí od konkrétního typu plnění, a to zejména následující:
 - a. 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 jeho dodávky a dále, že po celou dobu záruky bude mít parametry a vlastnosti požadované objednatelem;
 - b. prodloužená záruka – jedná se o záruku v intencích výše uvedené odrazky „záruka“ na dobu delší než standardní nebo obvyklou za dodržení parametrů a požadavků na záruku zařízení;
 - c. 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; jeli požadován u zařízení záruční servis a není-li jeho specifikace blíže upřesněna je požadován záruční servis Next business day on-site;
 - d. 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.
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. 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.
7. Pro hlášení servisních požadavků zajistí dodavatel zhotoviteli 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.

KABELOVÉ ROZVODY A DATOVÉ ROZVADĚČE

1. V ceně položky označené v Kalkulaci nabídkové ceny (vizte Příloha č.4 zadávací dokumentace) komodity **K5 – Kabelové rozvody LAN** jako „**Kabelové rozvody včetně příslušenství**“, jsou zahrnuty dílčí položky specifikované v samostatném výkazu výměr. Dodavatel v Kalkulaci oceňuje kabelové rozvody včetně příslušenství a datových rozvaděčů jako celek, položky v samostatném výkazu výměr slouží dodavateli pro kalkulaci celkové ceny této položky.
2. Dodavatel nacenění provede včetně záruky na kabelové rozvody v délce 10 let a záruky na rozvaděče v délce 24 měsíců.
3. Požadované provedení kabelových rozvodů včetně rozmístění datových rozvaděčů a dalších dodávaných technologií je uvedeno v projektové dokumentaci, kterou tvoří Příloha č. 2 **zadávací dokumentace**