# Technická dokumentace k veřejné zakázce „Zajištění vnitřní konektivity na OA KV“

## OBSAH DOKUMENTACE



## POPIS VÝCHOZÍHO STAVU

1. Areál Obchodní akademie, vyšší odborné školy cestovního ruchu a jazykové školy s právem státní jazykové zkoušky Karlovy Vary, příspěvkové organizace (dále jen škola) tvoří pětipodlažní (jedno podzemní a čtyři nadzemní podlaží) budova na adrese Bezručova 1312/17, 360 01 Karlovy Vary viz. obrázek. Školu navštěvuje 400 žáků.
2. Realizace projektu bude probíhat v celém objektu školy.
3. Současný stav ICT školy neodpovídá Standardu konektivity škol (dále jen Standard konektivity), a současným nárokům na výkon, bezpečnost a centralizovanou správu počítačové sítě. Počítačová síť byla budována postupně, stáří a technické úroveň používaných prvků je rozdílná. 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. roztříštěná 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. Kabelové rozvody v budově školy jsou provedeny kabely různých kategorií (Cat3-Cat5). Kabeláž není strukturovaná a nevyhovuje jednotnému standardu. Pokrytí budovy metalickými rozvody je nedostatečné a neumožňuje připojovat do sítě další zařízení (koncová zařízení, IoT a bezpečností prvky (kamery, rozhlas apod.)) a síť rozvíjet např. doplňováním WiFi přístupových bodů. 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 vkládacích 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.
5. Propojení stanic i serverů je zajištěno převážně přepínači 100 Mb/s (částečně i 1 Gb/s) bez možnosti pokročilé správy. Aktivní prvky jsou umístěné převážně v datových rozvaděčích a nejsou dostatečně zabezpečeny proti neoprávněné manipulaci. Škola nevyužívá 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 zajišťují společnosti O2 prostřednictvím spoje o rychlosti 125/25 Mbps. Rychlost připojení tak s určitou rezervou splňuje minimální požadavky Standardu konektivity škol (dále jen Standard konektivity) – 100 Mbps (400 studentů x 0,25 Mbps).

7. Škola má přiděleny veřejné IP adresy IPv4 a nemá IPv6. Škola nemá v současné době validující DNSSEC resolver na straně školy, neprovádí pokročilý monitoring provozu. Škola využívá dvě internetové domény - **oakv.cz** a **voskv.cz**
8. Škola provozuje spojení WiFi s omezeným pokrytím a nedostatečnou kapacitou pro připojení většího počtu klientských zařízení. Přístup zaměstnanců k síti je chráněna mechanismem WPA-PSK (sdílené heslo). WiFi je k dispozici zaměstnancům, studentům i hostům a partnerům. Síť není konsolidovaná, není 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 jen základní stavový firewall na bázi OpenWRT bez pokročilých bezpečnostních funkcí – např. IDS/IPS, URL filtrace, antivirové kontroly, aplikační kontroly, inspekce SSL provozu.
10. Škola provozuje 2 fyzické servery, jeden je virtualizován technologií Microsoft Hyper-V. Hardware serverů již není výrobci podporován a kapacitně i výkonově nepostačuje současným potřebám. Hlavním serverovým operačním systémem je Windows Server 2016, který je využíván pro sdílení souborů, zajištění základních síťových služeb (DNS, DHCP, provoz adresářové služba Active Directory a sdílených aplikací. Pro webové služby (aplikace Přijímačky a Termíny) jsou využity operační systémy Linux Ubuntu.
11. Zálohovaní dat a systémů je částečné a je prováděno prostředky operačního systému. Zálohy jsou ukládány na externí diskové úložiště. Zálohy nejsou chráněny proti poškození či kompromitaci cíleným útokem.
12. Hlavní softwarovou platformou serverů i uživatelských počítačů jsou operační systémy společnosti Microsoft. Na koncových počítačích učitelů i žáků 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 a jen omezeně hromadně/centralizovaně s výjimkou řízení aktualizací službou Microsoft WSUS (Windows Server Update Services).
13. Pro zajištění potřebných aplikačních licencí produktů Microsoft škola využívá licenční program Enrollment for Education Solution.
14. Škola využívá cloudové služby Microsoft 365 pro studenty i zaměstnance.
15. Škola využívá a prostřednictvím internetu vzdáleně zpřístupňuje ze své sítě webové aplikace BakaWeb, Suplování, Přijímačky a Termíny. Aplikace jsou dostupné prostřednictvím IPv4 šifrovaným protokolem https zabezpečeným certifikáty vydanými veřejnými certifikačními autoritami. Web školy je hostován u externí společnost a je publikován na IPv4 i IPv6 adresách šifrovaným protokolem https zabezpečeným certifikáty vydanými veřejnými certifikačními autoritami.
16. Školským informačním systémem je systém Bakaláři 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 | Automatizace procesů | 1 |
| K5 | Kabelové rozvody LAN | 1 |
| K6 | Koncová zařízení | 4 |

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. Přechod 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.
7. 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.
8. 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 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 WiFi

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 WiFi (a IOT) budou nasazeny moderní přístupové body (AP – access point) standardu WiFi 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 úrovní firewallu, tak aby bylo možné komunikaci podrobit kontrole za pomoci UTM nástrojů (min. AV, IPS, kategorizace obsahu) a mohl jí být přiřazen samostatný profil odlišný od profilů pro učitele a žáky. Ověřování přístupu do této VLAN bude zajištěno pomocí tzv. captive portálu – webové autorizace. Captive portál bude zajištěn firewallem případně jiným samostatným řešením nebo prvkem, ale vždy s důrazem na bezpečné oddělení uživatelského provozu od zbytku vnitřních sítí.
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 WiFi 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 WiFi 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 služby. 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 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 služby. 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.
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 uživatelovy jediné (centrální) identity. Správcem systému EDU je společnost Cesnet. V rámci projektu bude realizováno připojení do systému EDUROAM a bude nakonfigurováno připojení WiFi sítě do systému EDUROM prostřednictvím vybudované autentizační a autorizační platformy na bázi radius serverů a adresářové služby. Současně budou realizovány další netechnické požadavky pro provoz EDUROAM – např. vytvoření informační webové stránky, zajištění technického kontaktu apod. Zapojení do systému EDUROAM zajistí národní i mezinárodní mobilitu žáků a učitelů.
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 uchování informací v elektronické komunikaci spolu s požadavky Standardu konektivity škol a praktického pohledu na možné časové prodlení mezi vznikem incidentu a jeho vyšetřováním je definováno, že monitorovací a logovací systém bude umožňovat retenci dat min. 180 dnů. Na tento rozsah retence musí být dostatečně dimenzován 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 uživatelích (identitách) 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 organizace (např. nástup/výstup žáků), snížení chybovosti způsobené ručním zadáváním údajů do systémů a/nebo nedodržením 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 a § 20 Řízení přístupových oprávnění Vyhlášky č.82/2018 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

**K4 – Automatizace procesů**

1. Pro řízení správy celého prostředí a elektronizaci procesů školy bude pořízen systém uživatelské podpory typu Service desk. Systém bude podporovat řízení služeb podle standardu ITIL (Information Technology Infrastructure Library) – uznávaného souboru praxí prověřených konceptů a postupů, které umožňují lépe plánovat, využívat a zkvalitňovat využití informačních technologií, a to jak ze strany dodavatelů IT služeb, tak i z pohledu uživatelů. Fungování systému bude založeno na katalogu služeb vytvořeném v rámci dodávky, který bude možno dále rozvíjet a modifikovat libovolně podle požadavků škol a správců.
2. Součástí Automatizace procesů bude dále dodávka a implementace systému nebo modulu pro evidenci a správu prostředků (Asset management). Systém umožní evidenci jakéhokoli majetku či zařízení a svázání požadavků ze Service desku s konkrétním aktivem. Je požadováno, aby systém dokázal automaticky (bezagentově) detekovat hardwarové konfigurace a softwarové vybavení počítačů v síti a umožnil provádět softwarový audit.
3. 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 WiFi.

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 – Koncová zařízení**

1. V rámci komodity budou dodány a nainstalovány 4 koncová zařízení do nově vybudované infrastruktury.

## 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 výrobci 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<br>b. Implementace pořízených technologií<br>c. Analýza dat a stávajících sdílených systémů a jejich migrace na novou platformu<br>d. Návrh vhodné struktury adresářové služby, její vytvoření a naplnění identitami<br>e. Návrh a realizace zálohovacího řešení včetně nastavení zálohovacích plánů<br>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 Wi-Fi

a. Analýza stávajícího síťového prostředí a návrh nového architektury LAN i Wi-Fi
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 domén **oakv.cz** a **voskv.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 domén **oakv.cz** a **voskv.cz**
h. 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
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 skupinu 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 podpory 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

**CENTRÁLNÍ LOGOVÁNÍ**

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 zařízeni
    - automatizace kontrol monitorovaných systémů z pohledu chování, zranitelností, konfigurace apod.
b. Provedení souvisejících konfigurací monitorovaných systémů

**SPRÁVA IDENTIT**

a. 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 systémů 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<br>• kompletní implementace systémů podle předimplementační analýzy a prováděcí dokumentace<br>• 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<br>• návrh a provedení akceptačních testů, musí zahrnovat výkonové testy a prokázat plnou funkčnost integrací v obvyklých scénářích použití |
| K4: Automatizace procesů |
| a. Analýza životního cyklu požadavků a souvisejících procesů ve vztahu k řešeným oblastem<br>b. Návrh katalogu služeb včetně vhodného a logického členění struktury služeb v jednotlivých oblastech řešení<br>c. Návrh grafického rozhraní katalogu služeb včetně intuitivních piktogramů (ikon) jednotlivých služeb<br>d. Návrh vhodných pracovních postupů (workflow) pro řešení požadavků<br>e. Návrh konfigurační databáze pro zavedení do systému<br>f. Návrh způsobu automatické inventarizace koncových zařízení (počítačů a notebooků)<br>g. Návrh vhodného způsobu iniciačního zavedení evidovaného majetku (naplnění databáze)<br>h. Implementace systému dle provedených návrhů a doporučení výrobce<br>i. 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 |

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 nabídky, zadavatel může v průběhu zpracování Prováděcí dokumentace provést jejich upřesnění či rozšíření.
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 OA Karlovy Vary tvoří přílohu č. 8 zadávací dokumentace (je upřesněním 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 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** |
| **Virtualizační server 1x** | Provedení | rackové provedení max. 2U včetně výsuvných kolejnic a montážního materiálu do racku (datového rozvaděče). |
| | CPU | 1x procesor, maximálně 16 jader<br>Procesorový výkon dle https://spec.org/ minimálně:<br>SPECrate®2017_int_base 176 bodů<br>SPECrate®2017_fp_base 228 bodů |
| | RAM | 192 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 | Min. 5x 1.9 TB SSD 1 DWPD a 5x 8TB 7200 ot/min, všechny disky s rozhraním SAS min. 12 Gb a podporu výměny za provozu (hot-swap) |
| | Rozšiřitelnost | Min. 2 volné pozic 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 60režimu. |
| | LAN | Porty min. 2x 1GbE, 2x 10/25 Gb SFP28<br>Všechny NIC s podporou virtualizace – VMware NetQueue, Microsoft VMQ.<br>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 možnosti 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.<br>Podpora vícefaktorového ověřování (autentizace) a integrace s Active Directory<br>Monitorování a řízení spotřeby.<br>HTML5 rozhraní<br>Stavové informace na čelním panelu s výraznou indikací nestandardních a chybových provozní 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, redundance, min. Titanium specifikace dle 80 PLUS https://cs.wikipedia.org/wiki/80_Plus, dostatečný výkon pro plné osazení HDD |
| | 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 čisla serveru. |
| **SW licence operačních systémů** | Serverové operační systémy | 3 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 | 200 ks klientských licencí vázaných na zařízení k nabízeným operačním systémům |
| | Terminálové licence | 40 ks klientských licencí vázaných na uživatele pro využití funkcionality terminálových služeb (např. MS Remote desktop services) v nabízených operačních systémech |
| **UPS 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 |
| | Účiník | 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 |

| **Komodita K1 – Virtualizační platforma** | | |
|---|---|---|
| | 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 |
| **SW licence zálohovací software (sada)** | Licence | trvalá licence zálohovacího software pro nabízený server bez omezení počtu zálohovaných virtuálních serverů a objemu dat. |
| | Efektivita ukládání dat | integrovaná 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 zálohovanéno 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-maily atd.) |
| | Záruka | 60 měsíců včetně nároku na opravné a nové verze |
| **Síťové 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 | Síťové 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 8x 1GbE (min. 2x WAN) a 2x 10Gb SFP+, USB pro externí 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 kód | 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<br>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 kategorii 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 | 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 |
| | 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, antimalvare, antispam, aplikační kontrola, sandbox) |
| **Centrální přepínač 1x** | 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 |

| **Komodita K2 – Zabezpečení LAN a Wifi** | | |
|---|---|---|
| | 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 |
| **Přístupový přepínač 9x** | 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) | 5x přístupový přepínač – 48x 1 Gb RJ-45 PoE + 4x 10 Gb SFP+, 176 Gbps, min. 730W<br>4x přístupový přepínač – 48x 1 Gb RJ-45 + 4x 10 Gb SFP+, 176 Gbps |
| **WiFi přístupový bod vnitřní (AP) 44 ks** | Základní funkce | Přístupový bod (AP) standardu Wi–Fi 6 včetně montážního materiálu na strop |
| | Frekvence | min. 3 nezávislé radiové moduly činnost v radiovém pásmu 2,4 a 5 GHz současně, s podporou standardu OFDMA min. u 2 modulů |
| | Architektura | Homogenní 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 sítí) na 2.4 i 5 GHz současně, podpora přiřazení každého SSID do samostatné VLAN |
| | Zatížení | min. 300 přiřazených (asociovaných) klientů na radiový 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 |

| Komodita K2 – Zabezpečení LAN a Wifi | | |
|---|---|---|
| | 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 (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** | 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 |
| **Příslušenství síťových prvků** | SFP moduly | 36 ks modulů SFP+ 10 Gb, SM min. 1 km, včetně DMI diagnostiky pro nabízené přepínače, LC konektor<br>2x kabel 1xQFSP+ => 4xSFP+, 5 m pro nabízené přepínače a servery |
| | Patch kabely | 18 ks optický kabel SM s konektory LC-SC, délka 1 m<br>18 ks optický kabel SM s konektory LC-SC, délka 2 m |
| | Záruka | min 36 měsíců |
| **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 |
| | Účiník | 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 Systém řízení přístupu do sítě podle standardu 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 |
| | Kontexová 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. |

| Komodita K2 – Zabezpečení LAN a Wifi | | |
|---|---|---|
| | 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 infrastrucure) 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** |
| **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 zdrojí |
| | 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, zasílaní 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 úrovní sledování spuštěných příkazů (cmd, powershell), vyváření procesů, změny souborů, registrů a síťové komunikace. Včetně nástrojů pro detekci potenciálně nebezpečných aktivit (změna časových razítek souborů apod.) |
| | Detekce zranitelností | automatická kontrola zranitelnosti operačních systémů Windows, Linux a macOS a aplikací (host based vulnerability detection) |

| Komodita K3 – Centrální logování a Správa identit | | |
|---|---|---|
| | 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) využívajích 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, Firofox) a umožní přístup k datům a funkcím Systému i jeho správu a konfiguraci. |
| | Evidence aplikací a rolí | integrovaný registr aplikací a informačních systémů (souhrnně 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:<br>- události systému včetně webových služeb (aplikační log)<br>- změny entit evidovaných systémem a změny konfigurace systému (auditní log)<br>- synchronizace s napojenými systémy (synchronizační log)<br>- odeslané notifikace a upozornění (notifikační log)<br>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). |
| | 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. |

| Komodita K3 – Centrální logování a Správa identit | | |
|---|---|---|
| | 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 delegovánu. |
| | Obnovení hesla | IDM bude obsahovat samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživatele 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 zasílání 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 soubory 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:<br>- Plná synchronizace – prochází všechny objekty v IDM a synchronizuje je s odpovídajícími objekty daného systému<br>- Změnová synchronizace – synchronizuje jen změny od poslední provedené synchronizace.<br>- Simulační synchronizace – synchronizace vytvoří report očekávaných změn v napojeném systému (bez ovlivnění produkčních dat).<br>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<br>- Microsoft Active Directory<br>- Microsoft 365<br>- 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 – Automatizace procesů | | |
|---|---|---|
| **Část** | **Parametr** | **Popis povinného parametru** |
| **Systém uživatelské podpory Service desk** | Základní požadavky | Systém musí poskytovat alespoň následující funkčnost:<br>• Technologická podpora pro řízení interních služeb a procesů<br>• Podpora uživatelů<br>• Řízení externích dodavatelů IT služeb.<br>• Jediné centrální místo hlášení a řešení servisních požadavků |

| Komodita K4 – Automatizace procesů | | |
|---|---|---|
| | Podpora procesů dle ITIL | Systém musí pokrývat následující procesy a funkce dle doporučení ITIL:<br>• Service Desk<br>• Incident Management<br>• Request Fulfillment<br>• Change Management<br>• Service Catalog<br>• Asset and Configuration Management |
| | Implementované procesy a funkce | Z procesů ITIL, které musí navržený systém podporovat (viz výše), budou v rámci projektu realizovány procesy a funkce:<br>• Service Desk – řízení požadavků koncových uživatelů ICT služeb<br>• Incident Management – řízení rychlého řešení výpadků nebo nestandardních stavů v infrastruktuře.<br>• Request Fulfillment – standardní proces řízení požadavků na služby. Zpracovány budou služby:<br>- Mobilní telefony – včetně veškerých souvisejících podslužeb – de/aktivace roamingu, blokace/výměna SIM, žádost o datový balíček, ztráta zařízení, de/aktivace služeb, požadavek na přístroj či jeho opravu, obecné požadavky<br>- Počítače a koncová zařízení (tiskárny, skenery) – rozsah navrhne uchazeč dle „best practice“<br>• Change Management - standardní proces řízení životního cyklu změn, včetně předávání HW a SW s podporou schvalování.<br>• Service Catalog – vytvoření katalogu služeb pro naplnění výše definovaných požadavků |
| | Katalog služeb | Logicky a přehledně strukturovaný katalog služeb. Katalog bude ve stromové struktuře členěn na jednotlivé oblasti/kategorie (Správa majetku, IT, Lidské zdroje atd.) a každá oblast bude obsahovat samostatný podstrom. Počet oblastí a služeb nesmí být licenčně omezen. |
| | Služby | Pro každou službu v katalogu služeb musí být možno plně definovat vstupní zadávací formulář včetně tvorby vlastních položek. |
| | Uživatelská přívětivost | Katalog služeb bude uživatelům přístupný prostřednictvím uživatelsky přívětivého a intuitivního grafického rozhraní. Prostředí bude odpovídat moderním trendům a zvyklostem – přehlednost, rychlá orientace bez nutnosti čtení textů, využití piktogramů či ikon, kontextové nápovědy. Vhodné pro použití na mobilních (dotykových) zařízeních |
| | Automatické přidělení požadavku | Výběrem služby z katalogu služeb bude automaticky bez dalšího výběru či zadávání automaticky přidělena skupina řešitelů a parametry SLA (Service Level Agreement). |
| | SLA | SLA musí být automaticky přiděleno jako vlastnost dané služby kombinovaná s uživatelem – pro stejnou službu může být různým uživatelům automaticky přiděleno různé SLA. |
| | Nastavení priority | Podpora nastavení priority řešených požadavků. |
| | Lokalizace | Lokalizované uživatelské rozhraní. |
| | Reporty | Integrované generování a tisk reportů. |
| | Zasílání reportů | Podpora automatického zasílání reportů emailem. |
| | Šablony reportů | Podpora tvory a úprav předpřipravených šablon pro automatické reporty. |
| | Znalostní databáze | Integrovaná znalostní databáze s možností její aktualizace. |
| | Zabezpečený přístup | Zabezpečený přístup do aplikace včetně integrovaného přihlašování do uživatelského prostředí i konzol prostřednictvím účtu Active Directory, řízení oprávnění přístupu k informacím. |
| | Portál | Integrovaný portál pro zaměstnance (vidí své požadavky) a manažery/nadřízené (vidí požadavky podřízených). |
| | Active Directory | Nativní integrace se stávající Microsoft Active Directory pro správu uživatelů a oprávnění. Automatické přihlašování do aplikace. |
| | Metadata Active Directory | Automatické načítání vztahu zaměstnance a jeho nadřízeného. |
| | Integrace s nástroji pro správu pracovních stanic | Integrace s nástroji pro správu pracovních stanic (VNC, RemoteDesktop, apod.). |
| | Integrace s poštovními servery a klienty | Integrace s poštovními servery min. integrace s Microsoft 365 pro automatické vyčítání e-mailů a zakládání nových požadavků či nových záznamů k stávajícím požadavkům.<br>Integrace s mailovým klientem – umožní řízení celého životního cyklu požadavku od založení po potvrzení vyřešení a uzavření z prostředí Microsoft Outlook |
| | Integrace s majetkovým systémem | Požadavky bude při zadávání možno provázat s konkrétním majetkem ze Systému pro správu a evidenci prostředků (Komodita K3) předěleným uživateli. Požadavek bude evidován v evidenci historie Systému pro správu a evidenci prostředků. |
| | Pracovní postupy (workflow) | Podpora tvorby workflow pro řešení požadavků včetně požadavků typu nadřízený / podřízený požadavek |

| Komodita K4 – Automatizace procesů | | |
|---|---|---|
| | Skripty | spouštění vlastních skriptů v průběhu řešení workflow |
| | Automatizace | Podpora vytváření a spuštění akcí na základě událostí – vytvoření, úprava, zrušení požadavku. |
| | Pravidelné požadavky | Podpora tvorby šablon libovolných úkolů a plánování jejich pravidelného automatické zakládání. |
| | Eskalace, zastupitelnost | Podpora nastavení eskalačních pravidel a cesta, podpora nastavení zastupitelnosti řešitele |
| | Vyhledávání | Fulltextové vyhledávání napříč požadavky |
| | Pohledy | Podpora definování vlastních pohledů a filtry nad požadavky uživateli. |
| | Komplexní požadavky | Podpora komplexních požadavků – jeden požadavek automaticky generuje související další požadavky v závislosti na stavu vyplnění údajů v požadavku. Přehledná kontrola plnění požadavků. |
| | Plánování | Operativní načítání emailů z poštovního klienta (min. Microsoft Outlooku) a plánování schůzky nebo úkolu do kalendářů. |
| | Založení požadavku e-mailem | Podpora automatického založení požadavku strukturovaným e-mailem |
| | Export dat | Možnost exportu dat do Microsoft Word, Excel. |
| | Rozšiřitelnost | Systém musí být možno licenčně nebo standardními doplňkovými moduly (ne programovými úpravami) rozšiřitelný o možnost integrace s telefonní ústřednou |
| | API | Systém musí umožnit rozšíření pomocí otevřeného a dokumentovaným rozhraní API na bázi webových služeb v rámci poskytnuté licence. |
| | ITIL | Nabízená hlavní verze systému musí být certifikována na shodu se standardy/procesy ITIL. Plnění požadavku bude prokázáno certifikátem přiloženým k nabídce |
| | Licence | Systém bude licencován min. pro 40 uživatelů, kteří mohou zakládat a řešit (uzavírat) požadavky a 2 uživatele, kteří mohou řešit (uzavírat) požadavky 400 žáků (ti mohou jen zakládat, sledovat a doplňovat požadavky). Poskytnutá licence bude trvalá |
| | Záruka | Záruka včetně nároku na opravné verze min. 60 měsíců. |
| **Systém evidence a správy prostředků 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:<br>- Asset and Configuration Management<br>- Software Asset Management |
| | Implementované procesy a funkce | z procesu Asset and Configuration Management budou implementovány min. následující funkce:<br>- podpora správy konfigurační databáze, musí být uchovávána historie konfiguračních položek<br>- podpora automatizace zjišťování informací o konfiguračních položkách hardware<br>Z procesu Software Asset Management budou implementovány min. následující funkce:<br>- řízení životního cyklu spojeného se softwarovými aktivy<br>- automatické zjišťování informací o konfiguračních položkách software<br>- 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 výrobci 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 úrovní 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. |

| Komodita K4 – Automatizace procesů | | |
|---|---|---|
| | 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 |
| | Intuitivné 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 (nadřízený/podřízený) |
| | 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 včetně příslušenství** | 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 – Koncová zařízení | | |
|---|---|---|
| **Část** | **Parametr** | **Popis povinného parametru** |
| **Stolní počítač** | Provedení | Stolní počítač typu "All-in-one" |
| **All-in-one** | Displej | Dotykový 24" (min. viditelná plocha 23.8") IPS, antireflexní, s rozlišením FullHD (min. 1920 x 1080) |
| **4x** | CPU | výkon CPU dle https://www.cpubenchmark.net min. 13000 bodů |
| | Video | výkon video/grafického procesoru dle https://www.videocardbenchmark.net min. 1350 bodů |
| | RAM | 16GB DDR4, rozšiřitelná min na 32 GB |
| | HDD | min. 500 GB SSD, provedení PCIe M.2 NVMe |

| | | |
|---|---|---|
| | LAN | 1 Gb, standardní RJ-45 port |
| | Konference | integrovaná kamera min 720p (HD) s podporou přihlašování Windows Hello, integrované stereo mikrofony a reproduktory, |
| | Bezdrátové připojení | WiFi 6 802.11 ax, 2.4 + 5 GHz, anténní systém MIMO 2x2 pro vysokou propustnost<br>Bluetooth min. 5 |
| | Porty | Celkem min.6x USB, z toho 1x USB-C (10 Gb) a 1x USB-A (10 Gb + nabíjení) na čelním panelu nebo boku monitoru, ostatní porty min USB 3.2 (5 Gb/s)<br>1x HDMI/DisplayPort 1.4 výstup<br>Audio - sluchátka a mikrofon na předním panelu nebo boku monitoru |
| | Periferie | USB klávesnice se samostatným numerickým blokem a českým popisem<br>USB optická myš |
| | Bezpečnost | TPM 2.0 čip |
| | Software | Operační systém Microsoft Windows v aktuální verzi s podporou domény Active Directory, 64 bitový, české rozhraní |
| | Záruka | min. 36 měsíců poskytovaná výrobcem, oprava následující pracovní den v místě instalace |

## 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 (viz. Příloha č. 4b 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 odrážky „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 požadovanou 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 servisní požadavků zajistí dodavatel zhotoviteli přístup ke svému helpdeskovému systém 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 nabídky. 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 (viz. Příloha č. 4b zadávací dokumentace) komodity K5 – Kabelové rozvody LAN jako „Kabelové rozvody včetně příslušenství“, jsou zahrnuty dílčí položky specifikované v samostatné kalkulaci (příloha nazvaná – 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.
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. 2b **zadávací dokumentace - soubory** OA_KV_LAN_-1NP.pdf, OA_KV_LAN_1NP.pdf, OA_KV_LAN_2NP.pdf, OA_KV_LAN_3NP.pdf, OA_KV_LAN_4NP.pdf