1. Parametry technického řešení

1.1. Obecné požadavky

(1) Cílem projektu je zvýšení bezpečnosti a související modernizace IT infrastruktury, aby implementací projektu byly naplněny Standardy konektivity škol[1] (dále jen Standard konektivity) a rozšířena funkčnosti ICT prostředí základních škol zřizovaných Zadavatelem.

(2) Serverová infrastruktura bude virtualizována a provozována v TCORP s využitím všech jeho výhod (vysoká dostupnost, bezpečnost, zálohování, trvalý monitoring a správa).

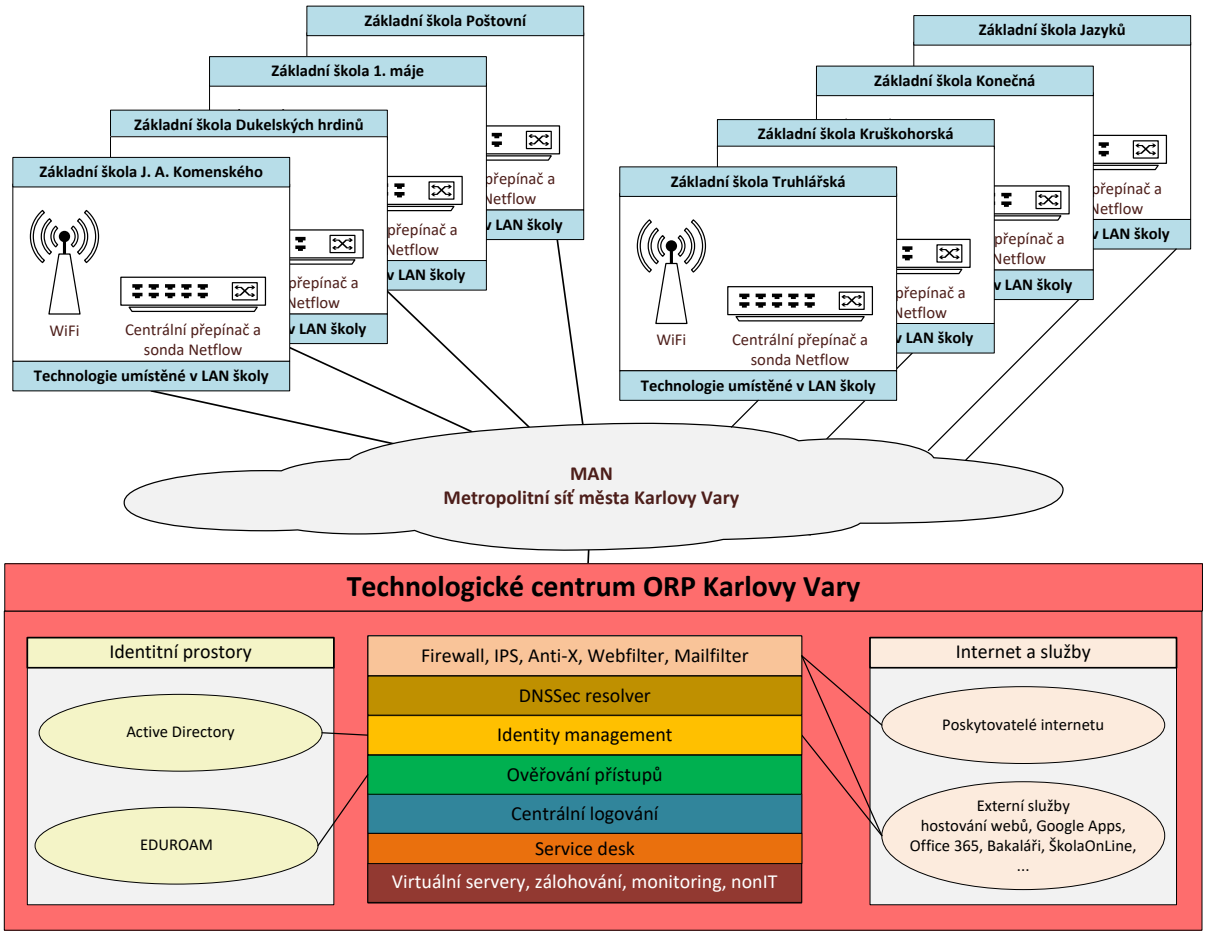
(3) Uchazeč bude při implementaci respektovat provozní řád zadavatele, vítězný uchazeč bude s provozním řádem seznámen před podpisem Smlouvy o dílo.

(4) Veškerá dokumentace vytvořená v rámci veřejné zakázky, musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. MS Office, PDF) používaných Zadavatelem na datovém nosiči a 1x v papírové formě. Papírová forma bude logicky a věcně strukturovaná, bude připravena pro použití (např. provozní dokumentace ve formě vhodné pro použití administrátory v serverovně). Struktura i forma dokumentace bude před předáním předána ke kontrole a výslovně schválena Zadavatelem.

1.2. Popis technického řešení

(1) Technické řešení konektivity škol bude založeno na synergickém využití již existujících technologií zadavatele – TCORP a metropolitní sítě města vybudovaných z prostředků IOP – a nových technologií pořízených v rámci tohoto projektu. Dojde tak k optimálnímu využití již investovaných prostředků zřizovatele a školy nebudou zatížené provozem a správou náročných serverových technologií – tu zajistí zřizovatel v rámci již nastavených a ověřených postupů a systémů Technologického centra a metropolitní sítě.

(2) Blokové schéma na následujícím obrázku představuje rozmístění a vazby jednotlivých systémů. Je patrné, že ve školách budou umístěny a provozovány jen technologie, které jsou nezbytné pro připojení koncových zařízení. Tím dojde ke zjednodušení školní ICT infrastruktury a školám budou minimalizovány provozní nároky. Současně dojde ke standardizaci a konsolidaci používaných systémů a technologií, která umožní dále snížit nároky na správu řešení a zjednoduší rozvoj ICT napříč školami:



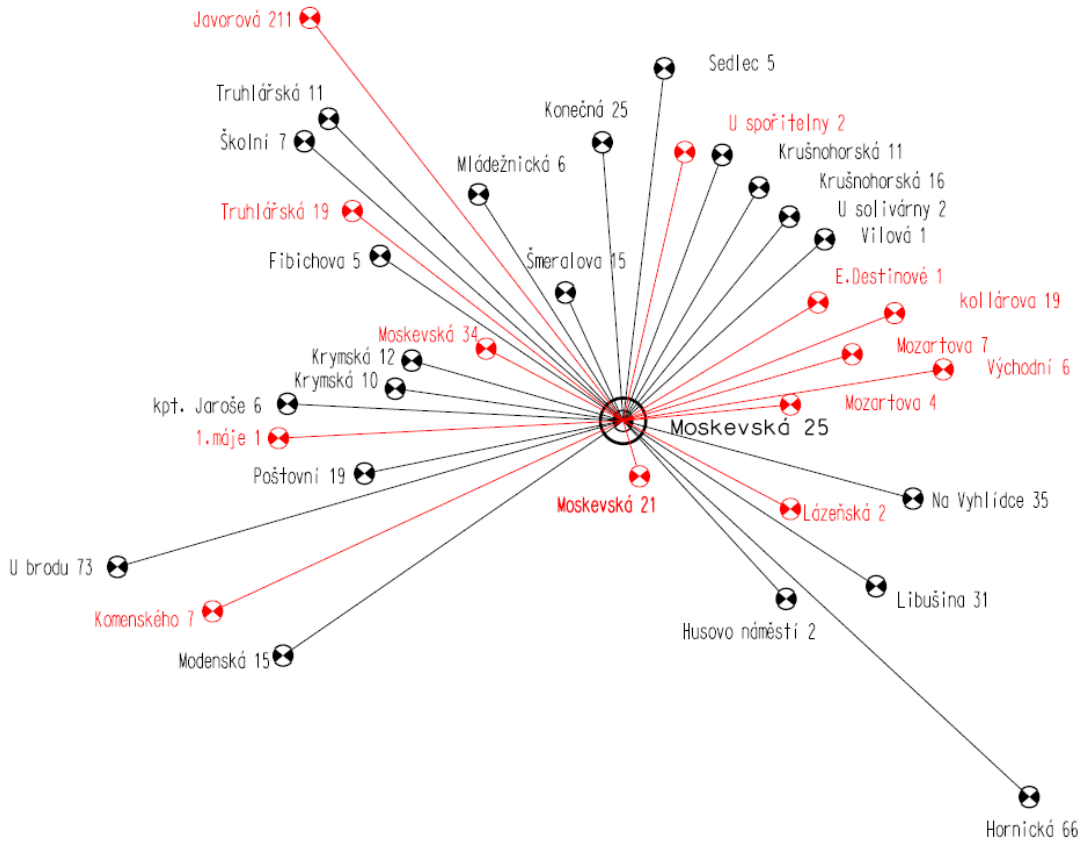
(3) V rámci předmětu plnění budou školy vybaveny (tj. budou umístěny ve školách) aktivními prvky LAN a WiFi.

(4) Pro sdílenou část řešení budou pořízeny technologie zajišťující centrální služby – servery s operačními systémy, diskové úložiště, systém pro centrální logování, vyhodnocování a správu událostí a bezpečnostních incidentů, identity management, systém uživatelské podpory, systém správy majetku, aplikační firewall, aktivní prvky LAN a zálohovací systém.

(5) Technologie zajišťující centrální služby budou umístěny v prostorech TCORP, protože se jedná o střed metropolitní sítě MMKV, na kterou jsou školy napojeny. Tyto sdílené technologie budou umístěny v prostorech TCORP také z důvodu maximálního využití stávajícího vybavení – záložního systém UPS a diesel agregátu, SAN a LAN infrastruktury, serverového šasi, klimatizace, zabezpečeného přístup a environmentálního a provozního monitoringu a vysoce dostupného clusteru UTM firewallu Fortigate – pro tento projekt tak není nutné vybudovat další serverovnu nebo další vhodný prostor, ale budou využity již existující prostory a technologie.

(6) **Sdílené technologie budou sloužit výhradně pro potřeby škol a fyzická zařízení budou označena pro snadnou identifikaci.**

(7) Metropolitní síť MMKV je navržena jako logická i fyzická hvězda s centrem na Magistrátu města (Moskevská 1281/21, Karlovy Vary). Jednotlivé přístupové lokality (tj. školy) metropolitní sítě jsou připojeny do tohoto centrálního uzlu s využitím optické infrastruktury. Centrum sítě je připojeno do stávající LAN MMKV a dále do internetu.



1.3. Specifické požadavky K1 – Virtualizační platforma

(1) Pro provoz veškerých pořízených systémů a aplikací budou pořízeny dva servery do stávajícího Blade šasi.

(2) Pro provoz systémů a aplikací budou pořízeny licence operačních systémů včetně nezbytných přístupových licencí.

(3) Pro virtualizaci pořízených serverů budou pořízeny rozšiřující licence stávajícího virtualizačního software.

(4) Pro ukládání dat budou pořízeny expanzní diskové police včetně pevných disků a současně budou pořízeny rozšiřující licence diskové virtualizace.

(5) Součástí virtualizační platformy bude vybudování aplikačního firewallu pro publikaci webových aplikací a systémů vzdáleného přístupu a správy.

(6) Pro zálohování bude v rámci projektu pořízeno síťové uložiště NAS s dostatečnou kapacitou pro ukládání provozních záloh a archivů logů systému Centrálního logování a SIEM. Zálohování bude řízeno pokročilým zálohovacím software, který bude prostřednictvím virtualizačního hypervizoru zálohovat všechny virtuální servery. Zálohovací systém umožní zálohovati i fyzické servery a osobní počítače.

(7) Pro zajištění bezpečnosti a možnosti řízení provozu v síti a zajištění prokazatelného monitoringu, logování a auditu interního i externího síťového provozu bude pro každou školu vybudována centrální databáze identit na bázi adresářové služby.

(8) Adresářová služby umožní ukládání a přehlednou správu identit (účtů včetně metadat) učitelů, žáků i externích subjektů, ale i technických prostředků – serverů, tiskáren, pracovních stanic.

(9) Adresářová služba bude poskytovat službu LDAP a umožní snadné napojení autentizačních mechanismů a protokolů – radius, agenta firewallu a dalších.

(10) Adresářová služba zajistí ověřování uživatelů pro účely jejich autorizace k přístupu k síťovým prostředkům (LAN, Internet) i výpočetním zdrojům (pracovní stanice, tiskárny, sdílené složky).

(11) Technické provedení adresářové služby bude založeno min. na 2 řadičích adresářové služby kvůli vysoké dostupnosti. Řadiče budou provozovány ve virtuálním prostředí a budou pravidelně automaticky zálohovány.

Součástí řadičů budou základní síťové služby – DNS, DHCP, obě v konfiguraci pro vysokou dostupnost. Ověřování identit bude 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.

Komodita K1 - Virtualizační platforma		
Část	**Parametr**	**Popis**
Virtualizační server **2 ks**	Provedení	**Blade server HPE BL 460c Gen10**
	Procesor	2x procesor osmi-jádrový **Intel Xeon Gold 6134**. Výkon serveru dle http://www.spec.org/ SPECint_rate_base2006 = 1030 bodů a SPECfp_rate_base2006 = 922
	Pevné disky	2x SSD, 240 GB pro hypervizor
	Paměť	384 GB RAM, 2666 MT/s
	Rozšiřitelnost	rozšiřitelnost RAM na 896 GB bez výměny RAM modulů
	RAID	řadič RAID 0,1, 10, zálohovaná vyrovnávací paměť pro zápis 1 GB
	LAN porty	LAN 2x10Gb s podporou iSCSI a virtualizace VMware NetQueue, Microsoft VMQ. Podpora partitioningu - rozdělení fyzického LAN adaptéru na více virtuálních adaptérů - 4 virtuální adaptéry na každý port
	FC porty	2x FC (fibre channel) port 16 Gb
	Vzdálená správa	Podpora vzdálené klávesnice, myši a obrazovky bez nutnosti běhu OS, možnost zapínat a vypínat server, možnost bootování se vzdáleného média.
	Kompatibilita	Podpora nejrozšířenějších operačních systémů (Windows, Linux) a hypervizorů (Hyper-V, VMware)
	Kompatibilita	Plně kompatibilní se stávajícím Blade šasi HP C7000 na fyzické i elektrické úrovni
	Vysoká dostupnost	Podpora a licence pro clusterový provoz
	Management	Plná integrace s management modulem HP Blade šasi HP 7000
	Záruka	Záruka 36 měsíců, oprava následující pracovní den v místě instalace
SW licence operačních systémů a databází	Operační systémy	2x **Windows Server 2019 Datacenter** 16 core (možnost Downgrade) Licence 64 - bitového serverového operačního systému v aktuální verzi pro nabízené servery. Licence umožňuje provoz neomezeného počtu virtuálních serverů stejné verze v prostředí stávající serverové virtualizace, dále provoz všech nabízených aplikací, management nástrojů a systémů.
	Klientské licence	**Windows Server Device CAL 2019** (možnost Downgrade) klientské licence pro nabízené operační systémy umožňující využívat těchto systémů uživatelům celkem na 1000 zařízeních.
	Databáze	**Microsoft SQL 2017 Standard** 4 core Databázový server v aktuální verzi umožňující vybudování databázového clusteru (active - passive) v licenčním režimu využívající 4 výpočetní jádra a umožňující využívání všech funkcí neomezenému počtu uživatelů. Server musí být datově a programově plně kompatibilní s databázovým serverem MS SQL server
	Licence	Uživateli licencí budou základní školy města Karlovy Vary, licence budou poskytnuty v licenčním programu Academic
Rozšíření diskových úložišť	Expanzní police	2ks **HP D2700 Disk Enclosure SFF** expanzní police pro rozšíření diskové kapacity pole HP MSA 2000 G3 včetně redundantních napájecích zdrojů a propojovacích kabelů. Kapacita police min. 25 disků 2,5“
	HDD 2,5"	50 ks HDD 600 GB / 15000 ot. SAS 12 Gb, dual port pro nabízené police
	Kompatibilita	Plná kompatibilita s diskovými poli HP MSA 2000G3
	Záruka	Záruka 36 měsíců s opravou v místě instalace
Rozšíření diskové virtualizace	Rozšíření	Licence **DataCore** pro rozšíření obslužné kapacity stávající diskové virtualizce SDS (software defined storage) DataCore s podporou FC (fibre channel) a Storage tiering
	Licence	Licence DataCore umožňují rozšíření obsluhované kapacity o 40 TB. Licence budou využívány základními školami města Karlovy Vary
	Záruka	Záruka 12 měsíců včetně nároku na nové verze
Rozšíření serverové virtualizace	Rozšíření	Licence **4x VMWare vSphere Ent Plus** pro virtualizaci nabízených serverů kompatibilní se stávající virtualizační platformou a umožňující správu stávajícími management nástroji. Licenci musí umožnit automatické přesouvání virtuálních serverů pro rovnoměrné zatížení serverů
	Licence	Licence budou využívány základními školami města Karlovy Vary, licence budou poskytnuty v licenčním programu Academic
	Záruka	Záruka 12 měsíců včetně nároku na nové verze
Rozšíření kapacity UPS	Rozšíření	Přídavný bateriový modul pro stávající UPS Eaton 9PX pro pokrytí potřeb nově pořizovaných technologií.
	Podpora	Bateriový modul je podporován výrobcem UPS

	Záruka	Záruka 36 měsíců
Aplikační firewall 1 ks	Publikace aplikací	**Citrix NetScaler Enterprise** pro bezpečné zpřístupnění webových aplikací, administrátorských aplikací a vzdáleného přístupu (technologie Remote desktop services)
	Zabezpečení aplikací	Zabezpečení publikovaných webových aplikací a rozhraní
	Řízení aplikací	Směrování klientů dle stavu a vytížení serveru na úrovni aplikace (L7 dle OSI modelu)
	Šifrování	SSL offload a akcelerace
	Routování	Podpora dynamických routovacích protokolů
	Loadbalancig	Rozkládání zátěže serverů aplikační virtualzace i obecných serverů - min. protokoly TCP, UDP, FTP, HTTP, HTTPS, DNS, SIP
	Zabezpečení aplikací	URL/HTTP rewriting
	Optimalizace	Optimalizace TCP provozu pro pomalé linky (redukce otevřených spojení, zkrácení odezev apod.)
	Autentizace	Podpora vícefaktorové autentizace (ověřování), min. pomocí SMS
	Ochrana	ochrana proti DoS útoku
	Monitoring	Monitoring provozu publikovaných aplikací včetně historie
	RDP	Integrovaná proxy pro zabezpečení RDP (Remote desktop protocol) - pro vzdálenou správu technologií
	VPN	integrovaná SSL VPN
	Výkon	Propustnost portálu min. 200 Mbit/s při SSL šifrování
	Záruka	Nárok na technickou podporu výrobce a nové verze min. 12 měsíců
SW licence zálohovacího software	Licence	4x Licence **Veeam Enterprise** zálohovacího software pro nabízené servery bez omezení počtu zálohovaných virtuálních serverů a objemu dat.
	Efektivita ukládání dat	Integrované technologie komprimace a deduplikace.
	Nároky na správu	„Bezagentové" řešení – bez instalace agentů do zálohovaných virtuálních serverů či aplikací
	Replikace	Možnost replikace virtuálních strojů na jiný virtualizační nod za chodu serveru
	Řízení replikací	Integrované řízení přechodu provozu na replikované servery (fail-over) a zpět (fail-back) včetě automatických zpětných dosynchronizací
	Ochrana dat	Provádění datově konzistentních záloh hlavních serverových aplikací – Microsoft SQL server, Active Directory, souborové systémy – bez nutnosti odstávky aplikace
	Integrita záloh	Automatické ověřování integrity zálohy spuštěním zálohovaného serveru přímo ze zálohy v izolovaném prostředí
	Podpora WAN	Možnost plnohodnotné replikace přes WAN pro replikaci virtuálních serverů do vzdálených lokalit
	Snapshoty	využívání snapshotů, zálohování pouze dat změněných od poslední úspěšné zálohy
	Kompatibilita	Podpora operačních systémů Windows a Linux v zálohovaných virtuálních serverech
	Uložiště záloh	Možnost ukládání záloh na diskový prostor, síťové úložiště a páskovou jednotku/knihovnu
	Ochrana úložiště	Nastavení maximální zátěže diskového úložiště při zálohování
	Podpora DR (disaster recovery)	Možnost nouzového spuštění zazálohovaného virtuálního serveru ze souboru zálohy bez nutnosti obnovy
	Správa	Vytváření a správa úloh (zálohování, obnova) pomocí průvodců
	Správa	Automatický reporting úspěšných i neúspěšných úloh
	Obnova dat	Běžné úlohy obnovy (obnovení souboru, databáze SQL, objekty Active Directory) provádět pomocí průvodců i na úrovni jednotlivých objektů (např. jeden účet Active Directory, jeden soubor) přímo do původního umístění
	Fyzické počítače	Integrované zálohování fyzických počítačů (klíčových pracovních stanic) a serverů s operačními systémy Windows a Linux. Bez omezení počtu zálohovaných systémů a objemu záloh. Pro tuto funkci je přípustné použití agentů.
	Reporty	Reporty včetně historie
	Záruka	Záruka 12 měsíců včetně nároku na opravné verze software
Síťové úložiště NAS pro ukládání záloh **1 ks**	Provedení	Synology RS2418RP+ Rack Station
		Synology RX1217RP - expanzní jednotka

		do racku (19"), 4RU, včetně montážního materiálu do racku
	CPU	výkon 2455 bodů dle https://www.cpubenchmark.net
	HDD	24 pozic pro HDD
	Hot-swap	Disky vyměnitelné za chodu.
	Kapacita	Osazeno 24x **WD4003FFBX Red Pro 256MB** 4TB HDD SATAIII/256 MB cache, 7200 ot./min - určené pro nonstop provoz v NAS či diskových polích, podporované výrobcem NAS. Nejsou přípustné disky určené pro jiné účely - desktop, DVR, NVR apod.
	Rozšiřitelnost	2x USB 3.0 pro připojené externích disků a dalších zařízení
	Konektivita	2x SFP+ a 4 x 1 GBit Ethernet port s podporou agregace linek, loadbalancingu a redundance.
	Výkon	Rychlost zápisu 650 MB/sec při RAID5 a SMB/CIFS (bez šifrování)
	Kompatibilita	Plná podpora Microsoft Hyper-V a Windows ADS a ACL.
	Komunikace LAN	Sıtove protokoly SMB/CIFS, WebDAV, iSCSI, SSH, SNMP, http/s
	UPS	Podpora korektního vypnutí signálem z UPS přes LAN při výpadku napájení
	Paměť	Paměť RAM pro systém a cache 4 GB
	Napájení	Redundantní napájecí zdroje
	Podpora SDD	Podpora SSD disků pro ukládání dat a s možností využití SSD jako čtecí a zápisové cache rotačních disků
	Bezpečnost	Integrované hardwarové šifrování AES
	SFP+	včetně 2x SFP+ modulu 10 Gb, singlemode, konektor LC a kabelů LC-LC 10 metrů
	Ochrana dat	Integrované typy ochrany dat RAID 1, RAID 5, RAID 6, RAID 10
	Záruka	Záruka 60 měsíců včetně HDD v místě instalace

1.4. Specifické požadavky K2 – Zabezpečení LAN a WiFi

(1) V rámci komodity budou do škol dodány a do připravených rozvaděčů a na připravenou kabeláž osazeny síťové přepínače a přístupové body WiFi. Prvky budou kompletně konfigurovány pro zajištění funkcionalit uvedených níže.

(2) 6 ks centrálních přepínačů bude osazeno a konfigurováno v TCORP jako protějšky centrálních přepínačů škol.

(3) V rámci komodity bude zřízeno bezdrátové propojení 2 budov ZŠ Truhlářská, budovy jsou vzdáleny cca. 500 m a je mezi nimi přímá viditelnost. Uchazeč zajistí dodávku a instalaci odpovídajících upevňovacích prvků dle nabízeného pojítka (stožáry, konzoly) a kabeláž pro připojení k LAN školy (max. 100 m jedno vedení, uložení kabelů do povrchových lišt).

(4) Pro každou koncovou lokalitu (tj. základní školu) bude implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby s využitím technologie 802.1X.

(5) Pro hosty a externí uživatele sítí všech základní škol bude zřízena samostatná VLAN (Guest VLAN), které bude komunikačně (min. L3 pravidla, ACL) oddělena od vnitřních sítí organizace. Tato VLAN bude mít své L3 rozhraní až na úrovní firewallu, tak aby bylo možné komunikaci podrobit kontrole za pomoci UTM nástrojů (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.

(6) Řízení provozu v LAN bude realizováno vytvořením VLAN (802.1Q), segmentací sítě s routováním (přepínáním) provozu mezi VLAN na úrovni centrálního přepínače s nastavitelnými ACL. Pro řízení provozu na úrovni kvality služeb bude k dispozici technologie QoS (Quality of Services). Pro zajištění vysoké dostupnosti služeb budou klíčové aktivní prvky propojeny duálními trasami s automatickým rozkládáním zátěže a převzetím služeb v případě výpadku jedné trasy.

(7) Architektura WiFi bude založena na řešení s centrální správou prováděnou virtuálním kontrolerem (řadičem), který bude součástí firmwarů přístupových bodů a bude konfigurován v režimu vysoké dostupnosti a zajistí automatické rozložení zátěže klientů, roaming mezi spravovanými přístupovými body a automatické ladění kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení.

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

(9) Ověřování přístupu do LAN bude realizováno protokolem 802.1X vůči adresářové službě prostřednictvím protokolů radius a P/EAP. Provozovaná zařízení (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 suplikantů (např. starší tiskárny, zařízení na bázi jednoduchých operačních systémů či firmware) bude použit jiný - dodavatelem navržený - vhodný způsob ověření. Neověřená zařízení nezískají přístup do sítě vůbec nebo jim bude zpřístupněna pouze VLAN s omezeným přístupem (Intranet). Spolu s ověřováním (autentizací) bude implementována i autorizace, tedy dynamické zařazení klientského zařízení nebo uživatele do určené VLAN.

(10) Ověřování přístupu do WiFi sítě bude realizováno na stejném principu jako LAN (tj. protokol 802.1X + radius). Wifi bude nabízet více SSID (učitelé, žáci, Guest), které budou obsluhovány samostatnými VLAN a budou napojeny na 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 s AES šifrováním a konfigurováno shodně pro obě frekvenční pásma. Výjimkou bude síť určená výhradně pro hosty (Guest WiFi), kde bude realizován tzv. captive portál zajišťující webovou autentizaci hostů pomocí přidělených účtů nebo za pomoci před-generovaných číselných kupónů. Preferován bude captive portál firewallu s tzv. lobby přístupem pro správu a generování účtů/kupónů ne-technickou osobou.

(11) DNSEC je bezpečnostním rozšířením překladu doménových názvů za pomoci digitálních podpisů DNS zóny a v ní vnořených záznamů. Díky tomuto rozšíření nelze podvrhnout, nebo jinak upravit, odpověď DNS serveru. DNSSEC dále vylučuje většinu známých praktik zneužití regulérních DNS serverů k útokům na třetí cíle. Významně tak zvyšuje bezpečnost a zajišťuje autenticitu odpovědí. Pro plné nasazení DNSSEC budou v rámci projektu realizována opatření ve dvou oblastech:

(a) **Externí zóna** – do externí zóny spadají domény všech škol (např. zskomenskeho-kv.cz) registrované v TLD (Top Level Domain) .cz, pod jejímiž DNS záznamy jsou publikovány služby na jmenných (NS) serverech externího registrátora, nikoliv na vlastním NS serveru. V rámci projektu budou ve spolupráci s registrátorem domény doplněny podpisy DNSSEC k používaným zónám a zároveň budou doplněny záznamy pro služby publikované skrz IPv6 adresy, viz výše v kapitole Připojení k Internetu. Pokud současný registrátor neumožní doplnění podpisů DNSSEC, bude zóna převedena k jinému registrátorovi.

(b) **Vnitřní validující resolver** – řešení zajistí bezpečný překlad DNS jmen na IP pro veškerá uvnitř připojená zařízení a to, vzhledem k vyžadovanému dual-stacku, shodně pro obě verze IP protokolu. Bezpečným překladem se rozumí DNS server (resp. 2 servery pro redundanci) jako součást sdílených služeb, který bude schopen za pomoci rozšíření DNSSEC ověřovat podpisy dotazovaných zón, resp. hash podpisy jednotlivých záznamů jako odpovědí na DNS dotazy vnitřních zařízení. Tento DNS server bude současně zajišťovat i překlady pro dosud nepodepsané externí domény a zóny.

(12) DNSSEC kontroly (tzv. validace) budou probíhat výhradně na DNS resolveru, tak aby nebyla nutná jakákoliv úprava konfigurace vnitřních klientů. Validující DNSSEC resolver bude konfigurován tak, aby se sám dotazoval výhradně tzv. ROOT serverů nebo jiných důvěryhodných DNSSEC serverů, které bude zároveň používat jako tzv. Trust Anchors. V rámci projektu bude validující DNSSEC resolver vytvořen jako funkční rozšíření nově instalovaných DNS serverů rolí v rámci nově pořízených operačních systémů.

(13) Externě zajišťované služby (web školy, Google Apps, ŠkolaOnLine, Office 365) budou ve spolupráci s poskytovateli či provozovateli těchto služeb nastaveny i pro publikaci na IPv6 adresách, pokud ještě publikovány nejsou. Pokud současný provozovatel neumožní provoz služby na IPv6, budou služby převedeny k jinému provozovateli.

(14) Publikované interní služby (školské informační systém Bakaláři a SAS, Moodle) budou publikovány na přidělených IPv4 a IPv6 adresách a bezpečnost přenášených informací bude zajištěna šifrováním pomocí SSL – webové rozhraní bude přístupné protokolem https.

(15) V rámci stávajícího clusteru firewallů bude školám nakonfigurován virtuální firewall (lze si představit jako samostatný firewall pro každou školu), který bude sloužit jako bezpečná brána připojující školu k internetu, resp. ke konektivitě poskytovatele s využitím technologie NAT dle RFC 2663. Firewall zajistí oddělení vnitřního a vnějšího provozu na základě tzv. zón a mezi nimi postavených komunikačních pravidel (ACL/xACL), tzv. politik. Firewall bude schopen blokovat nejčastější útoky typu odepření služby (DoS) a bude účinně blokovat podvržení adresy (spoofing).

(16) Firewall zajistí zosobnění žáků a zaměstnanců s jejich internetovými aktivitami napojením na účty v doméně adresářové služby tak, aby byla na firewallu neustále k dispozici aktuální vazba uživatel-IP adresa, případně i

zdrojový rozsah portů. Konfigurace politik firewallu a jeho jednotlivých rolí umožní pohodlnou práci s účty i skupinami adresářové služby namísto IP adres a to ve všech úrovních, tedy vč. kategorizace a filtrace provozu. Role politiky budou schopny pracovat minimálně s těmito objekty – IP/subnet, uživatel/skupina, typ zařízení/operační systém.

(17) Pro splnění požadavku Standardu konektivity škol na logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic atd.) bude realizováno napojením firewallu na adresářovou službu.

(18) Firewall bude schopen omezovat šířku pásma (tzv. rate limiting) ve vybraných komunikačních pravidlech libovolné politiky firewallu. Omezení bude možno aplikovat jen pro vybrané skupiny vnitřních uživatelů. Firewall tedy umožní rychlostní omezení určených komunikací, ale zároveň bude schopen jiné druhy komunikace naopak upřednostnit (prioritizovat).

(19) Kontrola webového provozu nešifrovaného i šifrovaného (protokoly http a https) je mandatorním požadavkem Standardu konektivity škol a firewall ji bude umožňovat spolu s další UTM funkcionalitou. Pořízený firewall umožní provádět shodně inspekci šifrovaných (SSL) spojení vybraných protokolů i jejich nešifrovaných verzí – minimálně protokoly HTTPS, SMTPS, POP3S, IMAPS, FTPS a inspekce na jejich výchozích portech. Pokud bude předkládán certifikát firewallem, bude platný a důvěryhodný ve vnitřní síti.

(20) Kategorizace a selekce obsahu bude odlišná v závislosti na uživatelské skupině – požadovány budou minimálně dva profily – žák (student) a učitel. V obou případech bude kategorizace a selekce prováděna na základě kategorií automaticky aktualizovaných v rámci aktualizací UTM. Veškerá varování uživatele v souvislosti s kontrolou obsahu bude v českém jazyce a formou zobrazené náhradní webové stránky (s upozorněním na pravidla využívání ICT a vysvětlení důvodu blokování). K dispozici bude možnost přesměrování uživatele na původní požadovanou stránku po stanovené době. V případě chybné blokace bude mít uživatel možnost požádat pohodlnou formou o uvolnění, resp. změnu kategorie stránky. Kategorizace a selekce obsahu bude prováděna i pro šifrovanou (https, SSL) verzi http protokolu.

(21) Identifikace útoků a IPS bude dalším využitým bezpečnostním prvkem stávajícího next-gen firewallu. Ochrana proti průniku (IPS) pracuje podobně jako antivirus na základě definic připravených výrobcem. Definice mají výrobcem nastavenu zároveň i výchozí akci, jak s identifikovanou komunikací naložit (blokace, monitorování, reset). Ve většině případů jsou výchozí akce plně vyhovující a lze důvěřovat výrobci firewallu, že v definicích použité výchozí akce jsou pravidelně revidovány a rozšiřovány o nově identifikované hrozby vč. jejich případně blokace. Zařazením profilů IPS do vybraných v komunikačních pravidlech firewallu bude zajištěna automatická blokace identifikovaného útoku bez nutnosti zásahu správce. Firewallem zaznamenané útoky nebo jim podobné nežádoucí komunikace se mohou dále odrazit v rekonfiguraci pravidel firewallu popřípadě ve filtračních (ACL) pravidlech na páteřním L3 přepínači, to však již bude vyžadovat zásah správce.

(22) Antivirová kontrola prováděná firewallem bude umožňovat konfiguraci dvou úrovní hloubky kontroly/rychlosti a vytvoření tzv. profilů, které bude možno dle potřeby uplatnit v jednotlivých komunikačních pravidlech (politikách) firewallu, dle druhu a povahy konkrétního pravidla. Antivirová kontrola bude aplikována i na šifrovaná spojení (https, SSL). Infikované soubory musí být možno odstranit či zablokovat.

(23) Vzdálený přístup formou zabezpečeného tunelu skrze internet bude sloužit především zaměstnancům školy k jejich práci z míst mimo metropolitní síť MAN a externím IT správcům. Zaměstnanci školy by neměli být omezováni technologicky, firewall umožňuje vytvoření tunelu zabezpečeného protokolem SSL nejlépe na výchozím portu tcp/443 a bude k dispozici multiplatformní klientská aplikace nebo nativní (reverse proxy) přístup skrze webový portál firewallu a jeho aplikace (SMB, RDP, SSH, HTTPS). Konfigurace VPN bude provedena tak, aby bylo možné bezpečně ověřovat uživatelské účty v adresářové službě a autorizovat je pro přístup na základě členství ve skupině adresářové služby. K tomuto účelu může být využit standardní RADIUS protokol nebo zabezpečený LDAP. Obojí může být konfigurováno jako role interního serveru, ovšem s důrazem na redundanci. Ověřování bude konfigurováno proti dvěma nezávislým serverům, nehledě na použitý protokol. K zabezpečení SSL komunikace (VPN) bude pořízen a na firewallu instalován a konfigurován certifikát typu wildcard vystavený některou veřejnou a důvěryhodnou certifikační autoritou (root CA), tak aby byl na straně uživatele považován za validní a platný. Certifikát bude též použit pro zabezpečení publikovaných služeb školy (např. webového portálu školského informačního systému).

(24) Publikace (zpřístupnění z Internetu) online služeb školy na adresách IPv4 i IPv6 bude zajištěna nově pořízeným aplikačním firewallem, který zajistí pokročilé bezpečnostní funkce pro publikaci aplikací – např. SQL injection, řízení dle http požadavku (GET/POST), IP reputace, XML zabezpečení, ochrana proti DoS, content rewriting, kontrola příloh apod. Účelem aplikačního firewall je zvýšit úroveň ochrany (především) webových aplikací (resp. jejich dat) před zneužitím zejména v případě, kdy sama aplikace není dostatečně zabezpečená – např. z důvodu vnitřní chyby, nevhodného návrhu, ukončení nebo nedostupnosti podpory výrobce či nedostatečné údržby. Školní aplikace pracují převážně s osobními údaji (žáků) – např. školský systém, stravovací systém – a mají velký počet

externích uživatelů (rodiče). Je proto nezbytné zajistit jejich nejvyšší možnou ochranu před zneužitím nebo odcizením osobních dat. Aplikační firewall dále zabezpečí publikovaná administrátorská rozhraní serverů.

(25) V rámci předmětu plnění bude pro zajištění bezpečnosti všech stávajících i nově pořízených počítačů škol a všech virtuálních serverů pořízen integrovaný antivirový systém zajišťující komplexní ochrany před škodlivým software – malware. Systém bude centrálně spravován a aktualizován.

Komodita K2 - Zabezpečení LAN a Wifi		
Část	**Parametr**	**Popis**
Centrální přepínač **14x**	**Společné parametry**	Společné parametry
	Základní parametry	HPE 5800 24G Switch L2/L3 přepínač v rackovém provedení 1U
	Propustnost	neblokovaná architektura, propustnost 200 Gb
	Agregace portů	podpora LACP
	Směrování	statické a dynamické routování, policy based routing
	Řízení provozu	víceúrovňový QoS
	VLAN	VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření
	Ověřování uživatelů a zařízení	podpora 802.1X
	Dualstack	plný IPv4 a IPv6 dualstack včetně směrování a QoS
	Pokročilé funkce	plná podpora MPLS a VPLS včetně L2 a L3 MPLS VPN
	Stohování	pokročilé stohování - 2 (a více) přepínačů ve stohu se chovají jako jeden z pohledu správy i připojených zařízení (8 zařízení ve stohu)
	Sledování toků	export síťových toků (Netflow nebo ekvivalent)
	Monitoring a správa	plná podpora CLI, SSH, SNMP 1-3, syslog, sFlow, RMON, web rozhraní
	Záruka	60 měsíců, oprava/výměna zařízení do 2 pracovních dnů po nahlášení závady, včetně nároku na opravné verze firmware
	Specifické parametry	Specifické parametry
	Porty	4 ks – celkem 8x 10 Gb SFP+, 24x 1 GbE
		7 ks – celkem 4x 10 Gb SFP+, 24x 1 GbE, 16x 1 Gb SFP
		3 ks - celkem 4x 10 Gb SFP+, 24x 1 GbE
Přístupové přepínače	**Společné parametry**	Společné parametry
	Základní parametry	L2 přepínač v rackovém provedení 1U
	Stohování	podpora stohování pro jednotný management (přepínače jsou stohovatelné vzájemně bez ohledu na provedení)
	Propustnost	neblokovaná architektura
	Agregace portů	podpora LACP
	Dualstack	IPv4 a IPv6 dualstack včetně podpory ACL a QoS
	VLAN	VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření
	Ověřování uživatelů a zařízení	podpora 802.1X
	Monitoring a správa	plná podpora CLI, SSH, SNMP 1-3, syslog, sFlow, RMON, web rozhraní
	Záruka	60 měsíců, odeslání náhradního zařízení max. následující pracovní den po nahlášení závady, včetně nároku na opravné verze firmware
	Specifické parametry	Specifické parametry
	Porty a propustnost	Typ 1: Aruba 2530 48G Switch 9 kusů - 48x 1 GB RJ-45 + 4x 1Gb SFP (nesdílené), 104 Gb/s
		Typ 2: **Aruba 2530 48G PoE+ Switch** 22 kusů - 48x 1 GB RJ-45 PoE+ + 4x 1Gb SFP (nesdílené), 104 Gb/s
		Typ 3: **Aruba 2530 24G Switch** 1 kus - 24x 1 GB RJ-45 + 4x 1Gb SFP (nesdílené), 56 Gb/s
		Typ 4: **Aruba 2530 24G PoE+ Switch** 21 kusů - 24x 1 GB RJ-45 PoE+ + 4x 1Gb SFP (nesdílené), 56 Gb/s

		Typ 5: **Aruba 2530 8G PoE+ Switch** 1 kus - 8x 1 GB RJ-45 PoE+ + 2x 1Gb SFP (nesdílené), 20 Gb/s
	PoE+	Výkon PoE+ přepínačů umožňuje napájení nabízených WiFi AP na 50% 1 GbE portech současně.
WiFi přístupové body (AP) **282 ks**	Základní funkce	Aruba IAP-305 (RW) Instant 2x/3x 11ac AP přístupový bod (AP) WiFi včetně montážního materiálu na strop
	Frekvence	činnost v radiovém pásmu 2,4 a 5 GHz současně, 2 radiové moduly
	Anténní systém	interní systém MIMO 3x3 (5 GHz) a MIMO 2x2 (2,4 GHz), optimalizovaný pro montáž na strop
	Přenosové rychlosti	SU-MIMO (5GHz) až 1300Mbps, MU-MIMO až 867Mbps. 2,4GHz MIMO až 300Mbps.
	Standardy	podpora 802.3at, 802.11n, 802.11ac, 802.1x včetně přiřazování do VLAN
	Řízení klientů	automatické směrování komunikace klientů z 2.4 GHz na 5 GHz (pokud klienti podporují obě pásma)
	Rušení	průběžná detekce non-WiFi rušení a spektrální analýza
	Multi SSID	podpora vysílání 8 SSID (WiFi sítí) současně, podpora přiřazení každého SSID samostatné VLAN
	Zatížení	250 přiřazených (asociovaných) klientů na radiový modul
	Porty	1x 1Gb, PoE s podporou standardů 802.3at a 802.3af
	Úsporné napájení	podpora standardu Energy-Efficient Ethernet (EEE), nebo obdobného pro úsporu energie - viz https://en.wikipedia.org/wiki/Energy-Efficient_Ethernet
	Řízení provozu	klasifikace a kontrola provozu, detekce obvyklých aplikací s možností určení priority nebo šířky pásma zvoleného provozu
	Řízení kvality služeb	automatické řízení kvality služeb (QoS) pro hlas a video
	Současná obsluha více klientů	Podpora MU-MIMO (Multi-User MIMO) - multi-user multiple input/multiple output
	Přenosové rychlosti	SU-MIMO (Single-User MIMO) min. 1300Mb, MU-MIMO 850 Mb
	Bezpečnost	Detekce cizích přístupových bodů zjištěných v LAN i v radiofrekvenčním pásmu
	Virtuální kontroler	Virtuální, vysoce dostupný kontroler obsažený ve firmware každého přístupového bodu. Umožňuje kompletní centrální správu WiFi infrastruktury a řízení jejího provozu včetně roamingu klientů.
	Monitoring a správa	plná podpora CLI, SSH, SNMP 1-3, syslog, web rozhraní
	Správa frekvenčního pásma	automatické dynamické přidělování kanálů a řízení výkonu přístupových bodů pro vyrovnané pokrytí a minimalizaci interference
	Záruka	záruka 60 měsíců včetně nároku na opravné verze firmware
Optické prvky	SFP+ moduly	16 ks modulů SFP+ 10 Gb, MM včetně DMI diagnostiky pro nabízený centrální přepínač, LC konektor
	SFP+ moduly	2 ks modulů SFP+ 10 Gb, MM včetně DMI diagnostiky pro HP Blade přepínač Virtual Connect Flex 10/10D , LC konektor
	SFP+ moduly	48 ks modulů SFP+ 10 Gb, SM 20 Km, WDM BiDi, včetně DMI diagnostiky pro nabízený centrální přepínač, LC konektory. 24 párů - 1270 a 1330 nm
	SFP moduly	64 ks modulů SFP 1 Gb, SM 20 Km, WDM BiDi, včetně DMI diagnostiky pro nabízený centrální přepínač, LC konektor. 32 párů 1310 a 1490 nebo 1550 nm
	SFP moduly	48 ks modulů SFP 1 Gb, SM 20 Km, WDM BiDi, včetně DMI diagnostiky pro nabízený centrální přepínač, LC konektor. TX/RX 1310/1490 nm
	SFP moduly	48 ks modulů SFP 1 Gb, SM 20 Km, WDM BiDi, včetně DMI diagnostiky pro nabízený distribuční přepínač, LC konektor. TX/RX 1490/1310 nm
	SFP moduly	144 ks modulů SFP 1 Gb, SM 20 Km, WDM BiDi, včetně DMI diagnostiky pro nabízený distribuční přepínač, LC konektor. 72 párů 1310/1490 nm
	Optické patch kabely	12 ks kabel MM s konektory LC-LC, délka 3m
		352 ks kabel SM s konektory LC-SC, délka 3m
	Záruka	36 měsíců
Bezdrátové pojítko **sada (2 zařízení - 1 spoj)**	Základní funkce	2x **B24 Mimosa B24** radiová jednotka PTP 24 GHz s anténou bezdrátové pojítko pro propojení budov školy
	Provedení	venkovní, umístitelné na stožár nebo zeď
	Frekvence	provoz v bezlicenčním radiovém pásmu >= 10 GHz
	Anténní systém	směrové paraboly včetně (radomových) krytů
	Přenosová kapacita	1 Gbps
	Dosah	1 km při přímé viditelnosti

	Bezpečnost	Šifrování přenášených dat, standard AES
	Porty	2 porty - datový 1 Gb a vyhrazený port pro správu
	Napájení	PoE nebo PoE+
	Legislativa	vyhovuje pro provoz v České republice dle platných nařízení a předpisů, součástí dodávky bude veškerá potřebná dokumentace pro legální provoz
	Ochrana	Obě strany budou doplněny přepěťovou ochranou datových a napájecích (PoE) přívodů
	Záruka	24 měsíců včetně nároku na opravný firmware
Bezpečnostní certifikát 8 ks	Popis	Hvězdičkový SSL (tzv. wildcard) certifikát veřejné certifikační autority pro zabezpečení služeb publikovaných do internetu. Kořenový certifikát certifikační autority bude standardně obsažen v běžných desktopových a mobilních operačních systémech a být automaticky aktualizován v rámci aktualizace operačního systému.
	Záruka	36 měsíců
Licence antivirového systému **1030 ks**	Bezpečnost	**Kaspersky Endpoint Security Select** ochrana před malware včetně ransomware, integrovaný firewall, ochrana před průnikem HIPS (Host based intrusion prevention), řízení a ochrana webového přístupu
	Správa	Centrální správa součástí dodávky
	Instalace	Centrální vzdálená instalace nabízeného produktu a odinstalace obvyklých antivirových řešení třetích výrobců včetně free verzí
	Správa aplikací	Řízení aplikací - centrální vzdálená instalace, povolení/zákaz spouštění
	Výměnná zařízení	Řízení přístupu (zákaz/povolen) k výměnným zařízením - USB flash/diskym CD/DVD
	Mobilní zařízení	Správa mobilních zařízení iOS a Android - omezení spouštění aplikací, řízení internetového přístupu
	Podporované operační systémy	všechny desktopové a serverové operační systémy Microsoft aktuálně podporované výrobcem, macOS, iOS a Android
	Záruka	12 měsíců včetně bezpečnostních aktualizací

1.5. Specifické požadavky K3 – Centrální logování a SIEM AlienValut

(1) Informace o provozu a potenciálních zranitelnostech informačních systémů umožní zavádění preventivních opatření a předcházení případným bezpečnostních incidentů.

(2) Zavedením systému školy také získají schopnost detekce bezpečnostních incidentů a informace pro jejich rychlejší a efektivnější řešení.

(3) Reporty systému budou sloužit pro přehlednou kontrolu stavu a chování informačních systémů a uživatelů za určité období (typicky 1 měsíc) a ke kontrole dodržování compliance („jednání v souladu s pravidly") organizace.

(4) Systém umožní provádění tzv. NBA (Network Behavioral Analysis), tj. automatického trvalého monitorování síťového provozu, stavu a činností sledovaných zařízení s cílem detekce (potenciálně) nebezpečného provozu, stavu či chování.

(5) Data uložená v systému a systémem archivovaná budou zajištěna a zabezpečena před neoprávněnou změnou i pro účely vyšetřování případného bezpečnostního incidentu.

(6) Implementace systému bude v provedena v souladu s § 23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí Vyhlášky č.316/2014 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti.

(7) Nabízené řešení umožňuje:

(a) monitoring a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení (ve spolupráci s firewallem)

(b) logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)

(c) 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 na úrovni rozhraní WAN, ideálně i LAN) a to bez negativních vlivů na zátěž a propustnost zařízeni s kapacitou pro uchování dat po dobu minimálně 6 měsíců.

(8) Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací – může se jednat o jediné zařízení, softwarový nástroj či appliance nebo o řešení složené z více samostatných a vzájemně

kompatibilních komponent. Zařízení umožní správu z jedné grafické konzole, přístupné nativně skrze https bez nutnosti instalace klienta. Ukládání všech informací do bude prováděno jedné databáze tak, aby bylo možno realizovat multikriteriální vyhledávání napříč informacemi z různých zdrojů (netflow a syslog).

(9) 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 na straně firewallu za pomoci jeho SSO agentů či logů a dalších přístupových a autentifikačních systémů (RADIUS logy). Dále budou získávány informace o překladu zdrojových, vnitřních IPv4 adres na externím výstupním rozhraní firewallu, kde bude prováděn NAT. Bude se tedy jednat o informace obsažené v NAT tabulce. Spolu s tím bude po stanovenou dobu možné zpětně dohledat i vnější provoz k vnitřnímu zařízení.

(10) Systém umožní plnohodnotnou práci se síťovými toky, jejich zpracování a archivace. Nástroje systému budou umožňovat i analytickou práci s přijímanými toky, a to i zpětně. Systém bude přijímat informace standardními, níže jmenovanými, protokoly, ze síťových zařízení a serverových systémů. Bude umožňovat uchování každého záznamu v jeho nezměněné podobě, ale zároveň bude schopný dávat jednotlivé události ihned do souvislostí a vyhodnocovat riziko a případné bezpečnostní události aktivně notifikovat, resp. reportovat. Řešení bude umožňovat příjem provozních informací a metadat těmito protokoly:

(a) Protokol NETFLOW – síťové toky budou exportovány z centrálního přepínače školy a z firewallu. Konfigurace flow exportu bude sladěna s konfigurací na straně příjemce – monitorovacího a logovacího nástroje (verze, porty apod.). Je požadovaný takový rozsah dat, který zahrne maximum možných toků jdoucích přes páteřní přepínač s důrazem na komunikace z/do externích sítí (WAN). Bude zpracováván tento rozsah informací - monitorování IP (IPv4 a IPv6) s obsaženou informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ).

(b) Protokolem SYSLOG budou exportovány veškeré provozní informace, logy, síťových zařízení včetně firewallu na všech úrovních sítě. Obsaženy budou veškeré informace, které zařízení loguje vč. informačních s důrazem na změny konfigurace, přihlášení odhlášení, stavy jednotlivých portů a výstupy z procesu ověřování 802.1X.

(c) LOG soubory – monitorovací a logovací nástroj bude načítat textové log soubory a v nich obsažené informace. Především se bude jednat o RADIUS log soubory. Tyto soubory budou obsahovat identitu uživatele a časy a stavy jeho žádosti o přístup. Bude se tedy jednat o kritické soubory.

(d) SQL databáze - pro případy, kdy budou logy uchovány v SQL databázích, bude monitorovací systém podporovat i načítání těchto logů.

(e) Windows Eventlog – důležitou schopností monitorovacího a logovacího systému je práce s Windows Event logem. Z hlediska bezpečnosti, záznamu přístupů a statistických a provozních informací se jedná o zásadní zdroj informací. Napojení na Windows Event log bude řešeno jako nativní nebo formou samostatného agenta či sondy nebo sensoru monitorovacího a logovacího systému. Možným zdrojem bude Security a System Eventlog všech serverů i pracovních stanic.

(11) 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 požadováno, že monitorovací a logovací systém bude umožňovat retenci dat 180 dnů.

Komodita K3 -Centrální logování a SIEM		
Část	**Parametr**	**Popis**
Logování a SIEM	Základní funkce	**AlienValut USM** Integrovaný systém zpracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware a sledování síťových toků a detekce anomálií
	Ovládání	Uživatelsky přívětivý přístup ke všem komponentám systému z jednotného grafického uživatelského rozhraní (GUI). Konfigurace, definice zdrojů logů, definice korelačních pravidel, tvorba reportů, řešení událostí a další běžné operace probíhají z jediné řídící konzole s jednotným GUI.
	Správa prvků	Automatické jednorázové i plánovatelné vyhledávání i ruční přidávání Prvků a detekce jejich typů a vlastností. Prvkem se rozumí hw i sw (např. OS) s IP adresou. Prvky jsou typicky zdroji dat - logů a událostí.
	Skupiny Prvků	Podpora zařazování Prvků do skupin/kategorií dle vlastností (typ, operační systém, dostupné služby, síť) i metadat (umístění, hodnota)
	Metadata Prvků	Možnost konfigurace metadat Prvku - hodnota, priorita a spolehlivost (věrohodnost) událostí
	Monitorování Prvků	Automatické monitorování stavu Prvku - dostupnost poskytované služby a základní dostupnost (odezva na ping)

	Vyhledávání Prvků	Víceparametrové vyhledávání a filtrování Prvků podle vlastností i metadat, export do souboru v běžném strojově zpracovatelném formátu (csv, xml)
	Vazby	Detekce síťových prvků standardními protokoly a mapovaní jejich vazeb
	Detekce zranitelností	Automatická ruční i plánovaná detekce zranitelností Prvků (i nezařazených) - porovnání stavu Prvků s databází známých zranitelností průběžně aktualizovanou výrobcem
	Profily zranitelností	Vestavěné i uživatelsky definované profily detekce zranitelností - definice typů zranitelností, které mají být kontrolovány.
	Autentizace	Podpora detekce zranitelností s i bez přihlášení (autentizací) ke kontrolovanému Prvku.
	Detekce průniku	Víceúrovňová detekce průniku (intrusion detection) - na úrovni sledování síťového provozu a na úrovní Prvků.
	Instalace agentů	Podpora vzdálené instalace ID agentů (intrusion detection) pro operační systémy Microsoft Windows
	Detekce průniku - assety	Monitoring a analýza uživatelských aktivit, logů, integrity souborů a registrů, rootkitů či obdobného škodlivého kódu
	Detekce průniků - síť	Analýza monitorovaných síťových toků a detekce anomálií indikujících možné narušení bezpečností politiky (NBA - Network Behavior Analysis)
	Detekce anomálií	Monitorování síťových toků technologií netflow (verze 5,9,10) či kompatibilní (ipfix, netstream) dle nabízených přepínačů.
	Síťové toky hypervizor	Podpora sledování síťových toků (netflow či kompatibilní) virtuálních síťových přepínačů VMware vSphere
	Viditelnost síťových toků	Viditelnost síťového provozu - zobrazení, prohledávání, filtrování síťových toků včetně historie
	IP reputace	Integrovaná služba aktualizovaná výrobcem ohodnocující reputaci a spolehlivost veřejné IP adresy s možností změny priorit událostí, alarmů. Reputace založena na detekovaných (aktivitách IP adresy (spam, skenování, phishing, distribuce malware, botnet.
	Protokoly	podporované protokoly min. syslog, windows events collection (pomocí agenta i bezagentově (WMI), snmp, s/ftp, nfs, cifs, netflow
	Ukládání logů	Bezpečné ukládání logů s řízeným přístupem v nezměněné (nefiltrované) podobě (tzv. raw logy)
	Zpracování logů	Centrální zpracování logů, jejich normalizace, korelaci, grafická interpretace a archivace, včetně logů generovaných samotným řešením
	Rozšíření logů	Vytváření vlastních atributů v událostech. Automatické doplňování atributů aktuálními hodnotymi z externího zdrojů. Podpora atributů v celém systému - vyhledávání, filtrace, korelace atd.
	Prohledávání logů	Pokročilé prohledávání a filtrování raw logů, podpora indexování pro zrychlení hledání
	Expirace logů	Podpora automatické rotace raw logů s nastavením doby expirace
	Zálohování logů	Podpora zálohování logů na externí síťové úložiště
	Ochrana logů	Zajištění integrity raw logů aplikací digitální podpisu. Možnost jednoduchého uživatelského ověření integrity
	Centralizace logů	Konsolidace logů na jednom centrálním místě.
	Geolokace	Automatické doplňování geolokačních informací k událostem a jejich grafické znázornění na mapě
	Doplňování názvů	Automatické doplňování reverzních DNS a hostname záznamů k IP adresám.
	Indentifikace MAC	Automatické doplňování výrobce zařízení podle MAC adresy
	Grafy událostí	Grafické znázornění událostí - četnost, typ, časová osa
	Parsery	Možnost vytváření uživatelských parserů bez nutnosti externí spolupráce
	Ladění parserů	On-line ladění uživatelsky vytvářených parserů v reálném čase- okamžité zobrazení rozparsovaných dat při vložení testovací zprávy/události.
	Standardizace logů	Standardizace přijatých logů do jednotného formátu, parsování parametrů do předepsaných polí
	Pohledy	Předpřipravené pohledy a podpora vytváření vlastních pohledů na data uživateli a jejich ukládání pro pozdější využití a zpracování dat. Včetně grafické reprezentace dat - grafy, mapy.
	Reporty	Integrovaný reportovací nástroj s přednastavenými obvyklými reporty a možností vlastních úprav a vytvoření nových reportů. Včetně grafické reprezentace dat - grafy, mapy.
	Upozornění	Zasílání uživatelsky vytvořených upozornění podle uživatelsky definovaných podmínek. Možnost zahrnutí přijatých rozparsovaných dat do upozornění.
	Správa uživatelů	Správa uživatelů systému je integrovatelná s MS Active Directory. Systém umožňuje i přihlašování pomocí lokálních účtů. Podpora granulárního (lokálního) nastavení uživatelských oprávnění
	Tikety	Možnost vytváření tiketů k bezpečnostním událostem s možností přiřazení řešiteli. Možnost sledování průběhu tiketů včetně historie - obsah, vykonané činnosti, eskalace. Podpora jednoduchého manuálního vytváření tiketů v průběhu vyšetřování incidentu.
	Automatizace tiketů	Tickety lze vytvářet automaticky na základě vytvořené policy k jednotlivým událostem / zranitelnostem.
	Politiky	Podpora vestavěných a tvorby vlastních komplexních politik zpracování událostí Politiky umožňují spustit následující akce: odeslání emailu, vytvoření ticketu, spuštění skriptu.

	Korelace	Podpora korelací události na základě definovaných parametru bez závislosti na typu zdroje. Vestavěné a výrobcem aktualizované korelace, podpora vytváření vlastních
	Rozšířené korelace	Systém umožňuje tvorbu korelací nejen napříč zdroji, ale také napříč daty z interních subsystémů (detekce zranitelnosti, průniků, IP reputace). V závislosti na datech interních subsystémů je případně upravena vážnost incidentu (oproti standardní korelaci).
	Upozornění	Podpora vytvářet upozornění (alertů) na základě korelovaných událostí včetně zahrnutí rozšířených korelací. Vestavěná upozornění i podpora ručního vytváření.
	IT Compliance	Podpora compliance (jednání v souladu s pravidly") - certifikace dle obvyklých bezpečnostních standardů a norem PCI DSS, HIPAA
	Auditní reporty	Vestavěné, výrobcem aktualizované šablony reportů pro podporů kontrolních a certifikačních auditů - dle standardů PCI DSS, HIPAA, NIST CSF, ISO 27001
	Legislativa	Systém zajistí bezpečné, úplné a nezpochybnitelné ukládání, vyhodnocování a archivaci logů ICT prostředí zadavatele a naplnění požadavků dle zákona č. 181/2014 Sb. (ZKB) a vyhlášky č.316/2014 Sb. (VKB), o kybernetické bezpečnosti, a to v platných zněních
	Provedení	Centrální část systému bude realizována jako jedna virtuální appliance
	Licence	Licence pro neomezený počet sledovaných systémů (Prvků), bez licenčního omezení velikosti aktivních i archivních dat či jiných funkcionalit systému.
	Výkon	Trvalé zpracování 1000 EPS (events per second - událostí za sekundu)
	Škálovatelnost	Možnost zvýšení výkonu doplněním dalších appliance pro sběr dat a vykovávání funkcí systémů, popřípadě rozdělením systému na více serverů.
	Vysoká dostupnost	Integrovaná podpora pro možnost doplnění dalšího systému (nodu) a sestavení clusteru – 2 systém, režim active/passive
	Záruka	12 měsíců včetně nároku na nové verze software a včetně aktualizací, bezpečnostní a funkčních signatur (zranitelnosti, korelační pravidla, detekce průniku, detekce Prvků (typy zařízení, aplikace, operační systémy), aktualizací reportů.

1.6. Specifické požadavky K4 – Systém uživatelské podpory a správy majetku ALVAO

(1) Pro řízení správy celého prostředí a koordinaci prací administrátorů škol a zřizovatele 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, který bude možno vytvářet a modifikovat libovolně podle požadavků škol a správců.

(2) Součástí Systému uživatelské podpory a správy majetku bude systém či modul pro evidenci a správu majetku (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 majetku bude umožňovat veškeré obvyklé operace s majetkem (pořízení, zavedení, převod, opravy, údržba, vyřazení) včetně tisku příslušných předávacích protokolů a automatického upozorňování na opakované události (revize, údržba, kalibrace). Pro správu IT majetku bude systém umožňovat obvyklé funkce softwarového auditu (přehled, přidělování, odebírání licencí a upozorňování na neoprávněně instalovaný software) v rozsahu akceptovaném hlavními výrobci software - např. Microsoft, Adobe, Autodesk.

K4 - Systém uživatelské podpory a správy majetku		
Část	**Parametr**	**Popis**
Systém uživatelské podpory **Service desk**	Základní požadavky	**ALVAO ServiceDesk** Systém poskytuje následující funkčnost: • Technologická podpora pro řízení interních služeb a procesů • Podpora uživatelů • Řízení externích dodavatelů IT služeb. • Jediné centrální místo hlášení a řešení servisních požadavků
	Podpora procesů dle ITIL	Systém pokrývá následující procesy a funkce dle doporučení ITIL: • Service Desk • Incident Management • Request Fulfillment

	• Change Management • Service Catalog • Asset and Configuration Management
Implementované procesy a funkce	Z procesů ITIL, které navržený systém podporuje (viz výše), budou v rámci projektu realizovány procesy a funkce: • Service Desk - řízení požadavků koncových uživatelů ICT služeb • Incident Management - řízení rychlého řešení výpadků nebo nestandardních stavů v infrastruktuře. • Request Fulfillment - standardní proces řízení požadavků na služby. Zpracovány budou služby: - 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 - Počítače a koncová zařízení (tiskárny, skenery) – rozsah navrhne uchazeč dle „best practice“ • Change Management - standardní proces řízení životního cyklu změn, včetně předávání HW a SW s podporou schvalování. • 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 vozového parku, IT, Lidské zdroje) a každá oblast bude obsahovat samostatný podstrom. Počet oblastí a služeb není licenčně omezen.
Služby	Pro každou službu v katalogu služeb je 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 bude 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.
Active Directory - metadata	Automatické načítání vztahu zaměstnance a jeho nadřízeného.
Integrace s nástroji pro správu pracovních stanic	Integrace s nástroji pro správu pracovních stanic (VNC, RemoteDesktop).
Integrace s poštovními servery	Integrace s poštovními servery, integrace se stávajícími servery (Office365, Google Suite) pro automatické vyčítání e-mailů a zakládání nových požadavků či nových záznamů k stávajícím požadavkům.
Integrace s majetkovým systémem	Požadavky bude při zadávání možno provázat s konkrétním majetkem ze Systému pro správu a evidenci majetku předěleným uživateli. Požadavek bude evidován v evidenci historie Systému pro správu a evidenci majetku.
Pracovní postupy (workflow)	Podpora tvorby workflow pro řešení požadavků včetně požadavků typu nadřízený / podřízený požadavek
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 (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 je licenčně nebo standardními doplňkovými moduly (ne programovými úpravami) rozšiřitelný o možnost integrace s telefonní ústřednou
	API	Systém umožňuje rozšíření pomocí otevřeného rozhraní API na bázi webových služeb.
	ITIL	Nabízená hlavní verze systému je certifikována na shodu se standardy ITIL 2011. Plnění požadavku bude prokázáno certifikátem způsobilé certifikační autority přiloženým k nabídce
	Licence	Systém bude licencován pro 100 uživatelů (pracovníků škol), kteří budou moci zastávat role zadavatelů i řešitelů požadavků a dále pro neomezený počet žáků – zadavatelů požadavků, které budou zpracovávány 16-ti řešiteli (2 pro každou školu).
	Záruka	Záruka včetně nároku na opravné verze 12 měsíců.
Systém správy majetku **Asset management**	Základní požadavky	**ALVAO Asset Management** 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 pokrývá následující procesy dle doporučení ITIL: - Asset and Configuration Management - Software Asset Management
	Implementované procesy a funkce	Z procesu Asset and Configuration Management budou implementovány následující funkce: - podpora správy konfigurační databáze, je uchovávána historie konfiguračních položek - podpora automatizace zjišťování informací o konfiguračních položkách hardware Z procesu Software Asset Management budou implementovány 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 vozidla, nemovitosti, vybavení kanceláří, pracovní prostředky a nástroje.
	Automatický sběr dat	Systém umožňuje 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 (organizační jednotky, skupiny uživatelů) v hierarchické struktuře. Struktura je volně upravitelná podle potřeb Zadavatele
	Řízení oprávnění	Systém umožňuje nastavit oprávnění na úrovní vlastností objektů - zamezit zobrazení pořizovací ceny uživatelům
	Rozšiřitelnost	Systém umožňuje přidávat do systému libovolné objekty a přidávat k těmto objektům libovolné vlastnosti.
	Dokumenty	V systému je možno ukládat libovolné elektronické dokumenty (faktury, licenční certifikáty) a tyto dokumenty propojit s konkrétním objektem nebo více objekty.
	Platnost dokumentů	Dokumenty je možno v systému zneplatnit (v systému zůstanou zachovány)
	Dědičnost	Systém podporuje 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 umožňuje automaticky evidovat změny provedené s jednotlivými objekty. Rozsah změn přesuny, instalace, předávací protokoly včetně informace kdo, kdy změnu provedl.
	Reporty	Systém umožňuje vytváření vlastních pohledů, filtrů a exportů 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 umožňuje automatické pojmenovávání spravovaných zařízení, min. pomocí definice (přednastavení) číselné řady.
	Řízení změn konfigurace	Systém umožňuje evidenci konfigurace systémů a zařízení.
	Vzdálená správa	Systém je možno integrovat s nástroji pro vzdálenou správu počítačů - 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 umožňuje rozšíření pomocí otevřeného rozhraní API na bázi webových služeb.
	Import	Systém umožňuje import majetku 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 je certifikována na shodu se standardy ITIL 2011. Plnění požadavku bude prokázáno certifikátem způsobilé certifikační autority přiloženým k nabídce
	Licence	Licence umožňuje spravovat 1000 počítačů a serverů a 20 000 ostatních aktiv. Poskytnutá licence bude trvalá
	Záruka	Záruka včetně nároku na opravné verze a aktualizace signatur pro rozpoznání hw a sw 12 měsíců.

1.7. Specifické požadavky K5 – Správa identit AC Identita

(1) V rámci komodity bude pro každou školu implementován systém pro správu identit (IDM – Identity management). Systém bude čerpat údaje o uživatelích (identitách) ze školského informačního systému příslušné školy a bude umožňovat doplňovat uživatele ručně, pokud nejsou v systému zavedeni.

(2) IDM bude na základě atributů uživatele (např. třída, doba studia) 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) tak, aby vždy odpovídalo nastaveným pravidlům a aktuálním atributům uživatele.

(3) Součástí systému pro správu identit bude detailní logování prováděných změn pro možnost zjištění uživatelských oprávnění v libovolném času v minulosti (od nasazení systému).

(4) 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 (nástup nových žáků), snížení chybovosti způsobené ručním zadáváním údajů do systémů a/nebo nedodržením procesů (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.

(5) Implementace systému bude v provedena v souladu s § 19 Nástroj pro řízení přístupových oprávnění Vyhlášky č.316/2014 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti.

Komodita K5 - Správa identit		
Část	**Parametr**	**Popis**
Systém pro správu identit (Identity management - IDM)	Základní funkce	IDM **AC IDENTITA** (dále IDM nebo Systém) bude udržovat a spravovat identity a organizační strukturu organizace - třídy, učitelský sbor, administrativa. Spravované identity budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy. Identity budou ukládány v databázi.
	Licence	Poskytnutá licence umožní nasazení a provoz IDM bez omezení na počet uživatelů, spravovaných identit a napojených systémů. Předpokládaný počet uživatelů je do 5000.
	Škálovatelnost	Systém umožňuje zvyšování výkonu (zlepšování odezvy) rozložením komponent Systému na více serverů - oddělení rolí (serverů) uživatelského rozhraní od výkonu integračních a provozních úloh.
	Evidence aplikací a rolí	Integrovaný registr aplikací a informačních systémů (souhrnně IS) a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby.
	Uživatelské role	Integrovaná správa uživatelských rolí, včetně zařazení uživatele do odpovídající role 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 intuitivní 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 (organizační jednotka, aplikační role, pracovní pozice).
	Logování SIEM	Systém bude poskytovat auditní logy pro pořizovaný logovací a monitorovací systém

	Logování systému	Systém obsahuje logování následujících typů událostí: - události systému (aplikační log) - změny entit evidovaných systémem a změny konfigurace systému (auditní log) - synchronizace s napojenými systémy (synchronizační log) - odeslané notifikace a upozornění (notifikační log)
	Správa identit	Systém bude spravovat organizační strukturu obsahující interní a externí identity jako samostatné větve struktury.
	Podpora eIDAS	Systém umožňuje implementaci procesů a rozhraní, která jsou vyžadována v Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.
	Požadavky na portál - obecné	IDM obsahuje webový portál (dále jen Portál), který bude sloužit jako hlavní rozhraní pro uživatele i správce pro přístup k datům, funkcím, správu a konfiguraci Systému.
	Správa referenčních objektů	Portál umožňuje přehlednou správu samostatných identifikovatelných objektů - referenčních objektů, na které se identity mohou odkazovat: pracovní pozice, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role.
	Referenční objekty	Systém umožní přidávání a správu dalších typů referenčních objektů a to i v průběhu správy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity
	Zabezpečení referenčních objektů	Systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů
	Rozšiřující 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.
	Přehledné 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).
	Vyhledávání - diakritika	Portál umožňuje vyhledávat i bez diakritiky (zadání Parizek vyhledává i Pařízek)
	Obrázky	Systém umožní k jednotlivým účtům (identitám) přikládat obrázky - fotografie.
	Ochrana proti chybám	Systém obsahuje mechanismus zabránění hromadným změnám z důvodu případných chybných vstupních dat (např. z personálního systému), aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v Active Directory apod).
	Aktivní uživatelé	Systém obsahuje přehled uživatelů aktuálně pracujících s Portálem
	Slučování identit	Systém umožňuje sjednocení více uživatelů (identit) do jedné a odpovídající sjednocení spravovaných účtů.
	Export údajů	Vestavěný export přehledů a seznamů zobrazených na portále do souborů CSV nebo obdobného strojově zpracovatelného a současně běžně čitelného formátu
	Filtrování	Vestavěný editor filtrů pro vyhledávání identit a referenčních identit. Možnost filtrování libovolných atributů identity včetně přidružených referenčních objektů. Možnost uložení filtrů pro opakované použití.
	Správa oprávnění	Víceúrovňová správa administrátorských oprávnění s možností nastavení oprávnění na úrovni organizační jednotky (nebo hlouběji) a detailní přiřazení rolí a oprávnění (přiřazení činnostní role, přiřazení aplikační role, editace identity)
	Granularita oprávnění	Oprávnění přidělovaná uživatelům a správcům je možné definovat a přidělovat pro jednotlivé části systému (identity, referenční objekty, notifikací, synchronizací, konfigurace systému, reporty, workflow, webové služby). U jednotlivých částí bude možnost definovat akce, které může uživatel s přidělenými oprávnění v konkrétní části IDM provádět.
	Správa licencí	IDM umožňuje spravovat licence pro jednotlivé evidované aplikace a přiřazovat je jednotlivým uživatelům (identitám). Pro schvalování přiřazování licencí bude IDM obsahovat workflow platformu s možností vytváření víceúrovňových schvalovacích workflow.
	Časová omezení	IDM umožňuje 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 umožňuje 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.
	Skupiny	IDM obsahuje správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i pracovní pozice.
	Delegování oprávnění	Možnost delegování administrátorských práv.
	Obnovení hesla	IDM bude obsahovat samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživatele je možnou provádět pomocí SMS (tj. IDM je možné na SMS bránu či službu napojit). Rozhraní umožňuje i běžnou změnu hesla (bez resetu).
	Individualizace	IDM umožní uživatelům individuálně nastavit vlastní zobrazení rozhraní - zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku - vždy pro každý seznam samostatně.
	Upozornění	IDM zajistí zasílání konfigurovatelných emailových upozornění pro následující události: vytvoření a změna identity, referenčního objektu (pracovní pozice, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role), problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu.

	Včasná upozornění	Upozornění na vypršení časových termínů je možno zasílat v předstihu. Velikost předstihu (např. 10 dnů) je možno konfigurovat pro každý typ upozornění samostatně.
	Šablony upozornění	Šablony upozornění umožňují definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám je možné nastavovat různé příjemce pro různé části organizační struktury (např. odbor, oddělení). Šablony umožňují vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu.
	Kontext upozornění	Pro zasílání jednotlivých typů upozornění je možno konfigurovat kontext, resp. podmínky, za jakých bude upozornění zasláno. V konfiguraci bude možné využít atributů identit a referenčních objektů. Příklad: notifikace budou generovány pouze pro identity v konkrétních uvedených skupinách, které mají uvedenu konkrétní aplikační role a konkrétní atribut atd.
	Logování	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 logování	Veškeré požadavky na změny v IDM je 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 ve formátu XML nebo CSV a budou obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IDM, aplikačních rolí, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti.
	Auditní report - výběr	Identity pro generování auditního reporty je možné vybrat (filtrovat) dle libovolných atributů identity včetně přidružených referenčních objektů.
	Reporty uživatelů	Vestavěné reporty obsahující uživatele s přímo přiřazenými aplikačními rolemi a s aplikačními rolemi delegovanými od jiných uživatelů. Reporty budou exportovatelný do CSV souboru.
	Reporty - historie	Automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení.
	Webové služby (WS)	IDM bude poskytovat rozhraní webových služeb pro napojení dalších systémů s možností konfigurace v Portálu.
	Standardy WS	Webové služby IDM 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.
	Logování WS	Volání webových služeb bude logováno a je možné je zobrazit v prostředí Portálu
	Služby rozhraní WS	Rozhraní bude poskytovat následující služby: - Získání organizační struktury - Získání hierarchie pracovních pozic - Získání seznamu identit - Získání nadřízené osoby pro daného zaměstnance - Získání seznamu aplikační rolí - Získání seznamu uživatelů dané aplikace - Zápis seznamu aplikačních rolí do IDM - Zápis a změna identit
	Synchronizace	Ruční i automatické spuštění synchronizací s propojenými systémy.
	Synchronizace - simulace	Spuštění synchronizací i v simulačním režimu pro ověření dopadu reálného spuštění bez ovlivnění produkčních dat a napojených systémů. Simulační logy budou zobrazitelné v Portálu.
	Simulace - průběh	Zobrazení jednotlivých stavů průběhu synchronizace bude k dispozici v přehledné grafické podobě.
	Synchronizace - režimy	Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM umožní IDM u každého systému využít více režimů synchronizací (za předpokladu podpory napojovaného systému): - Plná synchronizace – prochází všechny objekty v IDM a synchronizuje je s objekty daného systému - Změnová synchronizace – synchronizuje vždy jen změny od poslední spuštěné synchronizace. - Simulační synchronizace – synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka. - Historie běhu synchronizací – jednotlivé běhy synchronizací budou zaznamenány 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.
	Synchronizace - správa	Vestavěná 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. U jednotlivých synchronizací je možné vybírat organizace, které se mají z IDM synchronizovat s danými systémy. Správa bude součástí Portálu.
	Obecný konektor	Pro správu identit nenapojených aplikací a testování. Konektor simuluje aplikaci, požadavky na změny nastavení v aplikaci zasílá e-mailem správci aplikace. Podpora zpětné vazby - správce v IDM potvrzuje provedení požadavků pro účely logování

	Aplikační konektory	IDM bude spravovat identity a řídit oprávnění v dále vyjmenovaných systémech. V těchto systémech bude IDM vytvářet, aktualizovat, vytvářet uživatele a nastavovat jim oprávnění k rolím. - Microsoft Active Directory - Microsoft Office 365 - Google Suite - Moodle - nabízený Systém uživatelské podpory a správy majetku
	Zdrojový systém	IDM bude napojeno na školský informační systémy Bakaláři (www.bakalari.cz), ŠkolaOnLine (www.skolaonline.cz), iškola (www.iskola.cz) a EduPage (www.edupage.org). Z těchto systémů budou načítány údaje o organizační struktuře, osobách a tyto údaje budou pro IDM sloužit jako zdrojové
	Licence	Licence umožní spravovat neomezený počet identit na 8 základních školách města Karlovy Vary

1.8. Architektura technického řešení

(1) Architektura komodit je navržena tak, aby vhodně využívala a doplňovala stávající prostředky TC.

(2) Propojení mezi lokalitami (TC – školy) bude provedeno prostřednictvím stávající optické sitě MAN s komunikační rychlostí 10 Gb s využitím nabízených aktivních prvků (stávající prvky MAN budou nahrazeny).

1.9. Rozhraní

(1) Veškeré nabízené aktivní hardwarové produkty musí disponovat rozhraním SNMP min v2 pro management a vzdálenou správu.

1.10. Integrace

(1) Systémy komodity K4 budou integrovány - spravované požadavky bude možno při zadávání nebo kdykoli v průběhu řešení propojit s majetkem, jehož se požadavek týká.

(2) V systému bude dostupný přehled požadavků vztažených k evidovanému majetku s možností zobrazení detailů požadavku (klikacím odkazem do systému správy majetku).

1.11. Kompatibilita s ostatními systémy

(1) Veškeré softwarové komponenty nabízeného řešení budou provozovány ve virtuálním prostředí VMware vSphere a jsou pro běh v tomto prostředí výrobcem podporovány.

1.12. Typy klientů

(1) Řešení K1 (farma) umožňuje přístup k virtualizovaným aplikacím z operačních systémů Windows 7 a vyšších, OS X, Linux a mobilních zařízení s IOS, Android.

(2) Webové rozhraní systémů komodit K4 a K5 bude funkční v obvyklých internetových prohlížečích – Internet Explorer, Edge, Chrome, Firefox, Safari v aktuálních verzích

1.13. Bezpečnost informací

(1) Veškeré nástroje pro správu umožňují správu interních účtů (min. jméno a heslo) a/nebo napojení na Active Directory.

(2) Veškeré nástroje pro správu umožňují definici s 2 úrovněmi oprávnění – monitoring (pouze čtení), administrátor (plná správa)

(3) Veškeré nástroje pro správu komunikují se zařízeními šifrovanými protokoly (SSH apod.). Také v případě vestavěných nástrojů (např. www rozhraní hardware) je použita šifrovaná komunikace (např. HTTPS).

(4) Bezpečnost vnější komunikace publikovaných webových rozhraní aplikací a systémů bude zajištěna použitím tzv. „hvězdičkového“ (wildcard) certifikátu veřejné certifikační autority, tj. takové autority, jejíž kořenový certifikát je součástí běžných operačních systémů a je automaticky obnovován v rámci běžných updatů operačních systémů.

Hodnocené parametry	
Parametr	**Uchazeč popíše způsob naplnění tohoto hodnoceného parametru včetně značkové specifikace nabízených dodávek**
Snížení nároků na správu systémů	
1	Centrální přepínače komodity K1 budou založeny na systému Comware pro zachování jednotné správy LAN a MAN
2	Systém uživatelské podpory a správy majetku komodity K4 bude využívat pro ukládání dat centrální databázový server MS SQL TCORP
3	Systém pro správu identit komodity K5 bude využívat pro ukládání dat centrální databázový server MS SQL TCORP
4	Pro snížení nároků na správu síťové infrastruktury a zajištění její bezpečnosti poskytne uchazeč jednotný online nástroj pro poskytování technické podpory síťových prvků komodity K2 (tj. Centrálních přepínačů, Přístupových přepínačů a WiFi přístupových bodů (AP)). Nástroj bude disponovat následujícími funkcemi: 1) vyhledávání zařízení podle názvu a sériového čísla,

5	Pro snížení nároků na správu síťové infrastruktury a zajištění její bezpečnosti poskytne uchazeč jednotný online nástroj pro poskytování technické podpory síťových prvků komodity K2 (tj. Centrálních přepínačů, Přístupových přepínačů a WiFi přístupových bodů (AP)). Nástroj bude disponovat následujícími funkcemi: 2) možnost stažení aktuálního firmware a uživatelských příruček,
6	Pro snížení nároků na správu síťové infrastruktury a zajištění její bezpečnosti poskytne uchazeč jednotný online nástroj pro poskytování technické podpory síťových prvků komodity K2 (tj. Centrálních přepínačů, Přístupových přepínačů a WiFi přístupových bodů (AP)). Nástroj bude disponovat následujícími funkcemi: 3) ověření záruky a znalostní bázi známých problémů,
7	Pro snížení nároků na správu síťové infrastruktury a zajištění její bezpečnosti poskytne uchazeč jednotný online nástroj pro poskytování technické podpory síťových prvků komodity K2 (tj. Centrálních přepínačů, Přístupových přepínačů a WiFi přístupových bodů (AP)). Nástroj bude disponovat následujícími funkcemi: 4) možnost automatického zasílání upozornění na aktualizace firmware k pořízeným zařízením
Uživatelské přívětivost a snížení nároků na správu	
8	Kompletní uživatelské prostředí i prostředí pro běžnou správu a konfiguraci systému pro správu identit komodity K5 bude v českém jazyce
9	Systém bude integrován s MS Outlook. Integrací se rozumí rozšíření prvků MS Outlook (ribbon, formuláře a jejich ovládací prvky) o možnost plné správy požadavků přímo v prostředí MS Outlook.
Snížení nároků na provoz a rozvoj	
10	Pro minimalizaci nároků na provoz a rozvoj systémů komodity K4 bude dodána detailní uživatelské a administrátorské dokumentace (včetně popisů API a jeho použití) a dostupnost podpory výrobce (ne partnera) v českém jazyce. Dokumentace bude dostupná on-line.
Prokázání legislativní shody - Komodita K4	
11	Pro zajištění dodržování podmínek Usnesení vlády ČR č. 624/2001 - Pravidla, zásady a způsob zabezpečování kontroly užívání počítačových programů bude Systém pro správu majetku komodity K4 certifikován na shodu s tímto Usnesením oprávněnou certifikační autoritou. Tato skutečnost je doložena certifikátem způsobilé certifikační autority přiloženým k nabídce.

2. Implementační služby

2.1. Obecné požadavky

(1) Budou provedeny následující implementační práce na dodaných komponentech a případně dalších zařízeních. Implementační služby budou v následujícím rozsahu:

(a) Zajištění projektového vedení realizace předmětu plnění.

(b) Zpracování prováděcí dokumentace, která představuje projektovou dokumentaci, podle které se projekt bude realizovat. Součástí zpracování prováděcí dokumentace je mj. provedení předimplementační analýzy a zpracování finálního návrhu cílového stavu.

(c) Dodávku nabízených zařízení a kompletní implementaci řešení splňující povinné parametry technického řešení,

(d) Provedení školení,

(e) Zajištění zkušebního provozu,

(f) Provedení akceptačních testů,

(g) Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení a popisu činností běžné údržby a administrace systémů a činností pro spolehlivé zajištění provozu.

(h) Předání do plného provozu,

(2) Veškerá dokumentace bude zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standartních formátech (MS Office) používaných zadavatelem na datovém nosiči a 1x kopii v papírové formě.

(3) Činnost omezující práci uživatelů budou prováděny mimo běžnou pracovní MMKV, tj. mimo pracovní dny 7 – 17 hod.

K1: Virtualizační platforma
a) Návrh a kompletní provedení rozšíření serverové virtualizační platformy TCORP. b) Implementace pořízených technologií c) Analýza dat a systémů na stávajících serverech škol a jejich migrace na novou platformu d) Návrh vhodné struktury Active Directory s redundantními řadiči, její vybudování a migrace stávající pro každou školu e) Návrh a provedení rozšíření zálohovacího řešení f) Návrh a realizace konfiguračních změn infrastruktury (virtualizační platforma, LAN, SAN g) Návrh a realizace vhodného začlenění aplikačního firewallu do stávajícího prostředí, zejména koexistence se stávajícími firewally – vymezení rolí a pravidel, využití synergií. h) Návrh a provedení akceptačních testů, bude zahrnovat výkonové testy a testy vysoké dostupnosti
K2: Zabezpečení LAN a Wifi škol
a) Analýza stávajícího síťového prostředí a návrh nového architektury LAN i WiFi b) Implementace pořízených technologií včetně osazení aktivních síťových prvků (přepínače, WiFi AP, bezdrátové pojítko) na školách do připravených racků a na připravenou kabeláž (pasivní část LAN není součástí tohoto projektu). c) Provedení segmentace LAN – VLAN, adresování, routování d) Zavedení IPv6 pro přístup k internetovým zdrojům publikovaným na IPv6 adresách e) Zavedení IPv6 pro veškeré publikované služby škol z interních či externích prostředků. Včetně zajištění jednání a řízení změn u externích poskytovatelů služeb. Jde zejména o služby hostování domén škol, DNS, e-mail, web školy, webová rozhraní školských informačních systémů f) Zabezpečení komunikace publikovaných služeb pomocí nabízených certifikátů. g) Zavedení DNSSEC pro interní DNS služby i zabezpečení domén škol.

h) Návrh a implementace 802.1X pro kabelovou LAN i WiFi včetně uživatelské dokumentace pro konfigurace obvyklých zařízení a jejich systémů - PC, notebooky, chytré telefony, tablety, tiskárny - Windows, Linux, MacOS, Android, IOS, embedded systémy periferií

i) Návrh a provedení změn firewallu včetně vhodné virtuálních kontextů a konfigurací UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) pro všechny školy

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

a) Zajištění ostatních nezbytných činností pro naplnění Standardu konektivity

K3: Centrální logování a SIEM

a) Detailní identifikace zdrojů dat, jejichž provozně bezpečnostní informace bude nutné popř. vhodné sbírat, korelovat a analyzovat

b) Zdroje dat pro budou vybrány z tzv. primárních a podpůrných (technických) aktiv zadavatele. K jejich určení bude využito Vyhlášky č.317/2014 Sb. o významných informačních systémech a jejich určujících kritérií přiměřeně uzpůsobených a aplikovaných na prostředí zadavatele (zadavatel neprovozuje významný informační systém). Dále bude pro určení zdrojů dat využito vstupního osobního setkání (workshopu) se správci provozovaných informačních a komunikačních systémů v rozsahu jednoho pracovního dne.

c) Předimplementační analýza bude obsahovat následující oblasti specifické pro komoditu:
   1. specifikace profilu pro každý napojovaný zdroj dat, včetně určení vhodné úrovně detailu logování, odpovídající jeho roli v infrastruktuře,
   2. klasifikaci zdrojů informací pro stanovení priority události (stejná událost z různých zdrojů může mít různou prioritu) a z hlediska poskytovaných logů (obsažené informace, struktura logu),
   3. doporučení nastavení logování pro jednotlivé zdroje,
   4. výběr událostí a parametry jejich záznamů a metody sběru z jednotlivých zdrojů,
   5. návrh parserů pro zdroje, které nebudou systémem přímo podporovány,
   6. návrh doplňování logovaných informací z dalších zdrojů pro zlepšení jejich relevantnosti či srozumitelnosti,
   7. metody a pravidla identifikace, zpracování a vyhodnocování událostí, návrhy korelací,
   8. pravidla pro vznik varováni, upozornění, incidentů včetně priority,
   9. doporučenou strukturu oprávnění a řízení přístupových práv
   10. proaktivní a reaktivní procesy (aktivity, role, výstupy, doba odezvy) v případě výskytu varování, upozornění, incidentu a apod.
   11. popis zajištění autentičnosti logů,
   12. definice pohledů na události v konzoli uživatelů (např. setřídění událostí podle zdroje, typu, priority, stupně důležitosti, času vzniku apod.),
   13. návrh zálohování konfigurace a dat,
   14. návrh průběhu Zkušebního provozu pro ověření funkčnosti systému v reálném provozu,
   15. návrh retence logů a archivů,
   16. návrh způsobu napojení řešení na monitorovací systém uchazeče a definice procesů reakce, které jsou v souladu s platnou legislativou a bezpečnostní politikou škol,
   17. popis monitorovaných aktivit přispívajících k naplnění požadavků dle zákona č.101/2000 Sb. v aktuálním znění a k naplnění požadavků dle Nařízení evropského parlamentu a rady EU 2016/679 o Zabezpečení zpracování osobních údajů (GDPR),

d) 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

e) Návrh a provedení konfigurací dotčených a souvisejících systémů

f) Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy, testy archivace a obnovy logů a ověření detekce jejich neoprávněně modifikace.

K4: Systém uživatelské podpory a správy majetku

a) Analýza životního cyklu požadavků a souvisejících procesů ve vztahu k řešeným oblastem

b) Návrh katalogu služeb včetně vhodného a logického členění struktury služeb v jednotlivých oblastech řešení

c) Návrh grafického rozhraní katalogu služeb včetně intuitivních piktogramů (ikon) jednotlivých služeb

d) Návrh vhodných pracovních postupů (workflow) pro řešení požadavků

e) Návrh konfigurační databáze pro zavedení do systému

f) Návrh způsobu automatické inventaritace koncových zařízení (počítačů a notebooků)

g) Návrh vhodného způsobu iniciačního zavedení evidovaného majetku (naplnění databáze)

h) Implementace systému dle provedených návrhů a doporučení výrobce

i) Návrh a provedení akceptačních testů

K5: Správa identit

Předimplementační analýza bude obsahovat následující oblasti specifické pro komoditu:

a) provedení analýzy ICT prostředí škol se zaměřením na oblast správy uživatelských účtů, přidělování oprávnění a rolí,

b) technologický popis stávajících technologií s vazbou na systém správy identit

c) návrh životního cyklu identity uživatelů,

d) model organizační struktury,

e) přiřazení zaměstnanců a studentů k pracovním pozicím a rolím

f) atributy poskytované systémem školskými informačními systémy ve vazbě na řízené systémů a návrh jejich využití,

g) analýzu možností správy výstupních struktur,

h) analýzu evidenčních údajů a logů,

i) návrh a provedení akceptačních testů, musí zahrnovat výkonové testy a prokázat plnou funkčnost integrací v obvyklých scénářích použití

2.2. Zpracování prováděcí dokumentace

(1) Před zahájením implementačních prací bude zpracována prováděcí dokumentace, která bude důsledně vycházet z předimplementační analýzy a bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění.

(2) Jako podklad pro zpracování prováděcí dokumentace provede uchazeč předimplementační analýzu, která bude zohledňovat stávající prostředí zadavatele ve vztahu ke konkrétnímu nabízenému plnění, zejména pak s ohledem na použité technické řešení, pro následující oblasti:

(a) Detailní popis stávajícího stavu, identifikaci slabých míst a bezpečnostních rizik, včetně vazeb na HW a SW systémy TCORP.

(b) Způsob začlenění nabízených komodit do prostředí TC a škol.

(c) Síťová infrastruktura ve vztahu k plánovanému využití.

(d) SAN infrastruktura ve vztahu k plánovanému využití.

(e) Virtualizační infrastruktura (serverová, disková) ve vztahu k plánovanému využití.

(f) Integrace nabízených softwarových systémů.

(g) Rekonfigurace stávajících systémů.

(h) Dopady implementace na dostupnost a funkčnost stávajících služeb.

(i) Posouzení dopadů na non-IT technologie (spotřeba energií, tepelný výkon).

(j) Integrace s virtualizační platformou VMware vSphere ve vysoce dostupném režimu a integrace s dohledovým systémem Zadavatele
min. doporučení parametrů pro sledování).

(k) Požadované součinnosti Zadavatele a jejich rozsah.

(l) Návrh opatření k odstranění neshod zjištěných v průběhu analýzy.

(3) Prováděcí dokumentace zohlední podmínky stávajícího stavu, požadavky cílového stavu dle zadávací dokumentace a konkrétního technického řešení nabízeného uchazečem a bude obsahovat tyto části:

(a) Detailní popis cílového stavu včetně funkcionalit jednotlivých částí systému,

(b) Nutné a doporučené optimalizační a konfigurační změny dodávaných systému i všech navázaných systémů TCORP (vSphere, LAN, SAN atd.) a škol.

(c) Způsob zajištění potřebného HW a SW,

(d) Způsob zajištění koordinace realizace předmětu plnění s běžným provozem,

(e) Detailní návrh a popis postupu implementace předmětu plnění,

(f) Detailní popis zajištění bezpečnosti informací,

(g) Detailní harmonogram realizace včetně uvedení kritických milníků,

(h) Návrh designu síťového a bezpečnostního řešení a jeho konfigurace,

(i) Návrh designu aplikačních řešení,

(j) Vazby na stávající systémy a jejich konfigurace,

(k) Návrh akceptačních kritérií a akceptačních testů.

(4) Prováděcí dokumentace bude před zahájením realizace dalších etap plnění výslovně schválena zadavatelem.

(5) Prováděcí dokumentace bude před ukončením zkušebního provozu aktualizována dle skutečného stavu a následně bude součástí provozní dokumentace.

2.3. Harmonogram realizace

(1) Bude zajištěno projektové vedení po celou dobu realizace zakázky osobou odpovědnou za realizaci předmětu plnění, která bude hlavní kontaktní osobou a která bude přítomna při všech jednáních týkajících se projektu.

Č.	Etapa projektu – činnost	Zahájení etapy	Ukončení etapy
1	Předimplementační analýza a zhotovení Prováděcí dokumentace	D	D+30
2	Předání Prováděcí dokumentace Zadavateli, připomínkové řízení	D+30	D+40
3	Zapracování připomínek a předání finální verze Prováděcí dokumentace – akceptace Zadavatelem	D+40	D+50
4	Dodávky a implementace	D+50	D+190
5	Školení uživatelů a administrátorů	D+50	D+210
6	Akceptační testy	D+50	D+190
7	Zkušební provoz	D+50	D+210
8	Zahájení plného provozu a poskytování podpory provozu	D+210	-

2.4. Školení

(1) Uchazeč zajistí školení pracovníků Zadavatele – administrátorů – na zařízení a systémy, dodávané v rámci této veřejné zakázky, a to v rozsahu předávané provozní dokumentace.

(2) Školení zajistí seznámení pracovníků Zadavatele a škol se všemi podstatnými částmi díla v rozsahu potřebném pro provoz a údržbu implementovaných systémů.

(3) Rozsah školení je 40 hodin, z toho 4 hodiny pro každou školu.

(4) Školení bude probíhat v sídle Zadavatele a v lokalitách škol.

(5) Předpokládá se účast max. 4 administrátorů na každém školení

2.5. Provedení akceptačních testů, zkušební provoz a přechod do plného provozu

(1) Navrhneme způsob a provedení akceptačních testů. Akceptační testy budou pro všechny komodity vždy zahrnova:

(a) Prokázání kompletnosti dodávky a splnění povinných i hodnocených požadavků.

(b) Prokázání vysoké dostupnosti u řešení, která jsou takto koncipována.

(c) Prokázání aktivací software i hardware aktivačními klíči či jinými prostředky, je-li aktivace potřebná.

(d) Pro každou komoditu navrhne uchazeč vhodné doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost a odpovídající výkon a stabilita dodaného řešení.

(2) Povinným akceptačním kritériem pro akceptaci díla jako celku bude prokázání naplnění požadavků Standardu konektivity dle manuálu uveřejněného na http://www.irop.mmr.cz/cs/Ostatni/Web/Novinky/Zverejneni-doporucujiciho-manualu-k-postupum-pri-p včetně úspěšného provedení a doložení testu na https://www.standardkonektivity.cz/. Prokázání naplnění požadavků Standardu konektivity poskytne dodavatel v písemné formě vhodné jako příloha k Závěrečné zprávě o realizaci projektu.

(3) O provedení akceptace a jejím výsledku bude vyhotoven písemný protokol.

(4) Uchazeč zajistí zkušební provoz v délce 20 dnů včetně technické podpory 1 specialisty na dodané řešení s dojezdem do 2 hodin od nahlášení požadavku v pracovní den v době od 8h do 17h. V případě předávání díla po částech (viz bod (5)) je uchazeč povinen zajistit zkušební provoz (na vlastní náklady) pro předávané části díla až do doby zahájení plného provozu díla jako celku.

(5) Dílo lze předávat po částech následovně při dodržení následujících podmínek:

Komodita / Etapa	Etapa č. 4 – Dodávka a implementace	Etapa č. 7 – Zkušební provoz	Etapa č. 8 – Zahájení plného provozu a poskytování technické podpory
K1	V případě hardware dodání kompletního zařízení, v případě software dodání licencí. Provedení akceptačních testů alespoň v rozsahu bodu (1)(a), (c)	Provedení akceptačních testů alespoň v rozsahu bodu (1)(b), (d)	Provedení akceptačních testů v rozsahu bodu (2)

K2	-	Je možné předávat po jednotlivých lokalitách, je nutné provedení akceptačních testů alespoň v rozsahu bodu (1) (pro každou předávanou lokalitu)	Provedení akceptačních testů v rozsahu bodu (2)
K3	V případě hardware dodání kompletního zařízení, v případě software dodání licencí. Provedení akceptačních testů alespoň v rozsahu bodu (1)(a), (c)	Provedení akceptačních testů alespoň v rozsahu bodu (1)(b), (d)	Provedení akceptačních testů v rozsahu bodu (2)
K4	V případě hardware dodání kompletního zařízení, v případě software dodání licencí. Provedení akceptačních testů alespoň v rozsahu bodu (1)(a), (c)	Provedení akceptačních testů alespoň v rozsahu bodu (1)(b), (d)	Provedení akceptačních testů v rozsahu bodu (2)
K5	V případě hardware dodání kompletního zařízení, v případě software dodání licencí. Provedení akceptačních testů alespoň v rozsahu bodu (1)(a), (c)	Provedení akceptačních testů alespoň v rozsahu bodu (1)(b), (d)	Provedení akceptačních testů v rozsahu bodu (2)

(6) Při předávání díla po částech bude po předání jednotlivých částí a dokončení díla jako celku následovat zkušební provoz celého díla, akceptační řízení a předání celého díla včetně doložení prokázání plnění Standardů konektivity pro celé dílo podle kapitoly 3.1 Obecné požadavky, bod (1).

(7) Přechodem do plného provozu se rozumí okamžik úspěšné akceptace díla jako celku včetně vypořádání všech vad a nedodělků.

3. Záruky a servisní podmínky

(1) Záruka na veškeré dodané služby v délce trvání 3 měsíců a zařízení 24 měsíců (není-li u konkrétní komodity uvedeno jinak) od okamžiku ukončení implementace a předání do produkčního provozu.

(2) Není-li u konkrétní komodity uvedeno jinak, bude provedení záruční opravy do 5-ti pracovních dnů nebo poskytnutí náhradního prvku shodných nebo lepších parametrů po dobu opravy.

(3) Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně. Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro zadavatele.

(4) Uchazeč poskytne bezplatný (zahrnutý v ceně zakázky) přístup k aktualizacím software a firmware dodaných komodit po dobu záruky.

(5) Součástí technické podpory bude spolupráce s administrátory Zadavatele při řešení nekompatibilit aplikací a systémů.