Příloha č. 1 zadávací dokumentace - Technická specifikace zadavatele

Příloha č. 1 Kupní smlouvy - Technická dokumentace kupujícího

Obsah

[1 Technická specifikace zadavatele (kupujícího) 2](#_Toc160540655)

[2 Parametry pořizovaných technologií 4](#_Toc160540656)

[2.1 K1 – interní segmentační firewall 4](#_Toc160540657)

[2.2 K2 – patrový přepínač 48p s příslušenstvím (domov mládeže) 7](#_Toc160540658)

[2.3 K3 – patrový přepínač 8p PoE s příslušenstvím (domov mládeže) 8](#_Toc160540659)

[2.4 K4 – pavilonový přepínač s příslušenstvím (vychovatelé/domov mládeže) 10](#_Toc160540660)

[2.5 K5 - pavilonový přepínač s příslušenstvím (domov mládeže) 12](#_Toc160540661)

[2.6 K6 – optický páteřní přepínač s redundantním zdrojem a příslušenstvím 15](#_Toc160540662)

[2.7 K7 – přepínač 24p PoE s příslušenstvím pro wifi 18](#_Toc160540663)

[2.8 K8 – přepínač 12p PoE s příslušenstvím pro wifi 20](#_Toc160540664)

[2.9 K9 – licence SW pro řízení přístupu do sítě 802.1x 22](#_Toc160540665)

[2.10 K10 – WiFi přístupový bod s příslušenstvím 22](#_Toc160540666)

[2.11 K11 – licence SW pro řízení přístupových oprávnění – Identity management system 27](#_Toc160540667)

[2.12 K12 – Licence SW ochrany koncových stanic a serverů před škodlivým kódem (ANTI-X) 31](#_Toc160540668)

[2.13 K13 – licence pro správu kryptografických prostředků 33](#_Toc160540669)

[2.14 K14 – Zálohovací server s příslušenstvím 33](#_Toc160540670)

[2.15 K15 – Licence SW pro zálohování nově pořizovaných serverů 35](#_Toc160540671)

[2.16 K16 – NAS s příslušenstvím 39](#_Toc160540672)

[2.17 K17 – licence SW serverového operačního systému 39](#_Toc160540673)

[2.18 K18 – server pro hyperkonvergovanou infrastruktur (HCI server) s příslušenstvím 40](#_Toc160540674)

[2.19 K19 – Licence virtualizačního SW 42](#_Toc160540675)

[2.20 K20 – UPS s příslušenstvím 42](#_Toc160540676)

[2.21 K21 – Rack s příslušenstvím 44](#_Toc160540677)

[2.22 K22 – Appliance pro analýzu bezpečnostní událostí 46](#_Toc160540678)

[3 Instalace a zprovoznění 48](#_Toc160540679)

[3.1 Popis instalačních služeb 48](#_Toc160540680)

[3.2 Dokumentace 52](#_Toc160540681)

[3.2.1 Prováděcí dokumentace 52](#_Toc160540682)

[3.2.2 Provozní dokumentace 52](#_Toc160540683)

[3.3 Zaškolení IT administrátorů 52](#_Toc160540684)

[3.4 Přílohy 52](#_Toc160540685)

# Technická specifikace zadavatele (kupujícího)

Zadavatel požaduje dodávku jednotlivých komponent dle této technické dokumentace včetně příslušenství v níže uvedené minimální specifikaci.

Musí se jednat o zařízení nová, nepoužitá, nerepasovaná a určená pro prodej v České republice.

Součástí dodávky níže uvedených technologií budou i dále uvedené služby.

Součástí dodávky bude dále dodávka dokumentace a nezbytné zaškolení administrátorů v prostředí kupujícího k běžnému provozu a ovládání dodaných technologií včetně specifik a konfigurace provedené v prostředí kupujícího.

Nabízené zboží musí být standardní, běžně dostupné a určené k produkčnímu použití.

Není dovoleno použití beta-verzí, kódu s custom úpravami či neoficiálních verzí.

Veškeré nabízené zboží musí být pokryto oficiálním supportem, přičemž požadavek na provedení bezplatného servisního zásahu musí být možné kdykoliv vznést přímo na výrobce zařízení.

Veškeré deklarované funkce a technické parametry nabízeného zboží musí být dostupné nejpozději dnem podání nabídky.

Deklarované funkce a technické parametry nabízeného zboží musí být ověřitelné prostřednictvím oficiálních datasheetů, release notes či manuálů vydaných výrobcem.

Užité pojmy níže:

* NBD – další pracovní den, tzn. například realizace opravy zařízení nejpozději další pracovní den od nahlášení
* x BD – x pracovních dnů, tzn. například realizace opravy zařízení nejpozději poslední pracovní den dané lhůty od nahlášení
* on-site – realizace například opravy zařízení v místě dodávky

Z důvodu kompatibility se stávající infrastrukturou a proškolených správců počítačové sítě, mohou být v zadávací dokumentaci uvedeny konkrétní značky výrobků, nebo určitý výrobce. Důvody pro konkrétní značky výrobků jsou vždy uvedeny v konkrétní části specifikace tam, kde dochází k uvedení konkrétního produktového názvu. V souladu s § 89 odst. 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, zadavatel připouští možnost dodávky rovnocenného řešení, které však musí zajistit celý komplex služeb, který je kompatibilitou vyžadován, tedy komplexní řešení agendových informačních systémů nad touto platformou vybudovaných a provozovaných, které předmětnou infrastrukturu užívají a slouží k výkonu činností zadavatele.

V případě, že se tato dokumentace odkazuje na přílohu s označením „**NDA**“, jedná se o „Popis stávajícího technologického prostředí“, který bude poskytnut na základě podpisu smlouvy o ochraně důvěrných informací.

**Propojení zařízení – SFP moduly a kabely**

Všechny dodané technologie musejí být v rámci dodávky propojeny odpovídajícím způsobem a technologií, tedy zejména pro všechny síťové karty jednotlivých zařízení musejí být dodány i SFP a obdobné moduly a kabely do serverovny kupujícího, které takové propojení v kvalitě požadované u každého ze zařízení umožní. V případě 10Gbit karet musí být dodány SFP prvky a kabely umožňující využití této maximální rychlosti karty, v případě jiných rychlostí toto pravidlo musí být dodrženo stejně.

**Plnění jednotlivých komponent dle specifikace níže je požadováno v následujícím rozsahu, a to včetně příslušenství**

|  |  |  |
| --- | --- | --- |
|  | Položka | Počet |
| K1 | Interní segmentační firewall s příslušenstvím | 2 |
| K2 | Patrový přepínač 48p s příslušenstvím (domov mládeže) | 20 |
| K3 | Patrový přepínač 8p PoE s příslušenstvím (domov mládeže) | 20 |
| K4 | Pavilonový přepínač s příslušenstvím (vychovatelé/domov mládež) | 2 |
| K5 | Pavilonový přepínač s příslušenstvím (domov mládeže) | 2 sady |
| K6 | Optický páteřní přepínač s redundantním zdrojem s příslušenstvím | 1 sada |
| K7 | Přepínače 24p PoE s příslušenstvím pro wifi | 5 |
| K8 | Přepínač 12p PoE s příslušenstvím pro wifi | 6 |
| K9 | Licence SW pro řízení přístupu do sítě 802.1x | 1 |
| K10 | WiFi přístupový bod s příslušenstvím | 73 |
| K11 | Licence SW nástroje pro řízení přístupových oprávnění – Identity management system | 1 |
| K12 | Licence SW ochrany koncových stanic a serverů před škodlivým kódem (AntiX) | 1 |
| K13 | Licence SW pro správu kryptografických prostředků | 1 |
| K14 | Zálohovací server s příslušenstvím | 1 |
| K15 | Licence SW pro zálohování nově pořizovaných serverů | 1 |
| K16 | NAS s příslušenstvím | 1 |
| K17 | Licence SW serverového operačního systému | 3 |
| K18 | Server pro hyperkonvergovanou infrastrukturu (HCI server) s příslušenstvím | 2 |
| K19 | Licence virtualizačního SW | 1 |
| K20 | UPS s příslušenstvím | 2 |
| K21 | Rack s příslušenstvím | 3 |
| K22 | Appliance pro analýzu bezpečnostních událostí | 1 |

# Parametry pořizovaných technologií

## K1 – interní segmentační firewall

Firewall musí splňovat následující technické požadavky:

|  |  |
| --- | --- |
| Parametr | Popis minimálního parametru / funkcionality |
| Základní technické požadavky | Požadujeme platformu postavenou na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekryptace, porovnávání se signaturovou databází). |
| Celá dodávka musí obsahovat všechny HW komponenty a licence. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány. |
| Požadujeme dodání zařízení ve formátu HW appliance o velikosti max. 1RU, hloubky max. 35 cm a veškeré příslušenství (montážní prvky) pro montáž do RACKu |
| Dodané řešení musí umožňovat rozšíření platformy o další kus NGFW, jehož cílem bude zajišťování sdílení telemetrických informací, vizualizace stavu sítě, zařízení a klientů, přičemž cele řešení musí být podporováno výrobcem |
| Řešení musí umožňovat rozšíření platformy pro sběr logů a grafického reportingu včetně oboustranné komunikace (tím se rozumí minimálně odeslání a zpětné načítání logů pro účel vizualizace), nabízené řešení musí prokazatelně garantovat podporu této funkcionality. |
| HW parametry | min 16× Počet síťových rozhraní copper RJ45 10/100/1000 |
| min. 8× Počet GE SFP |
| min. 4× 10GE SFP |
| min. 1× Konzolový port pro management |
| min. 1× dedikovaný port RJ45 pro management |
| min. 1× USB 3.0 port pro zálohu konfigurace, případně pro připojení USB 4G modemu |
| Redundantní napájecí zdroj |
| Výkonnostní parametry | Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 27000 Mbps, 27000 Mbps, 11000 Mbps, latence firewallu (64 B UDP paket) - max 5 mikro sec, počet naráz otevřených spojení – min 3 M, počet nových spojení za sekundu - min. 280 000, počet firewall pravidel až 10 000, podpora virtualizace (min 10 virtuálních kontextů), |
| Základní funkce | Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IPsec SAs mezi nody v clusteru |
| Režim fungování L2 – transparentní režim, L3 – NAT/Router |
| Podpora VLAN |
| Podpora multicast, vytváření politiky pro multicast routování |
| Podpora 802.3ad link aggregation |
| Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading |
| Podpora centrální NATovací tabulky, stavová inspekce SCTP komunikace |
| Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP |
| Policy-based routing |
| Funkce SD WAN – možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky |
| VPN funkce | Funkce SSL VPN: podpora klientského i bezklientského (portálového) režimu, minimální počet současně navázaných SSL VPN tunelů 500, minimální propustnost SSL VPN 2000Mbps |
| Funkce IPSEC VPN: podpora site-to-site VPN, podpora klientských VPN, dostupnost VPN klienta pro koncové stanice (Windows, MacOS), funkce klientských IPSec VPN nesmí být licencovaná na počet uživatelů. V opačném případě požadujeme dodání neomezené licence, minimální počet IPSEC VPN tunelů typu lokalita-lokalita 2000, minimální počet klientských IPSEC VPN tunelů 16000, propustnost IPSec VPN (512 byte) min. 13 Gbps (měřeno při AES256-SHA256), podpora konfigurace redundantních IPSec VPN tunelů za pomoci statického směrování, podpora konfigurace redundantních IPSec VPN tunelů za pomoci dynamického směrování, podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace, podpora VXLAN, podpora L2TP, PPTP, GRE, podpora dynamických routovací protokolů OSPF, BGP ve VPN IPsec |
| UTM | Funkce detekce aplikací na L7 (Application Control) |
| Funkce detekce a potlačení narušení (IPS/IDS) |
| Funkce antivirové kontroly |
| Funkce kategorizace webových stránek |
| Funkce DNS filtru |
| Funkce ochrany před únikem citlivých informací (DLP) |
| Pokročilé funkcionality | Možnost nastavovat firewall politiku na základě geografických údajů |
| Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem |
| Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud |
| Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru |
| Viditelnost do provozu na aplikační úrovni |
| Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo) |
| Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu |
| Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření |
| Traffic Shaping, QoS s podporou prioritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii |
| Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu |
| Podpora funkce reverzní proxy |
| Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů |
| Explicit proxy | podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP), podpora transparentního ověřování uživatelů proti MS AD protokolem Kerberos, funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta, funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatel na terminálovém serveru |
| Virtualizace | Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů atp. |
| Součástí dodávky musí být licence na min. 10 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech) |
| Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů) |
| Management | FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici |
| Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě (je definován v příloze podléhající NDA) |
| Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury) |
| Záruka, servis a technická podpora | Záruka 60 měsíců, servisní zásah následující pracovní den od nahlášení závady, v místě instalace. Servis je poskytován výrobcem firewallu.  Technická podpora výrobce v délce 60 měsíců spočívající zejména v nároku na aktualizační balíčky zranitelností, opravné balíčky a patche, podpora bude uhrazena současně s dodávkou. |
| Příslušenství | 4x Modul SFP+ 10G-BASE-LR , 4x optický patch kabel 1m |

## K2 – patrový přepínač 48p s příslušenstvím (domov mládeže)

|  |  |
| --- | --- |
| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění požadované minimální funkcionality/vlastnosti** |
| Typ přepínače | L2/L3 přepínač |
| Formát přepínače | Stohovatelný |
| Počet portů 10/100/1000 Base-TX | 48 |
| Uplink porty | 4x1GE SFP |
| Min. velikost sdíleného systémového bufferu | 6MB |
| Velikost MAC address tabulky | 16000 |
| IEEE 802.3ad (Link Aggregation) | ANO |
| IEEE 802.3ad přes více přepínačů ve stohu nebo více šasís | ANO |
| Minimálně 8 linek jako součást Link Aggregation Group trunku | ANO |
| Minimální počet konfigurovatelných Link Aggregation Group trunků | 48 |
| IEEE 802.1Q | ANO |
| Minimální počet aktivních VLAN | 1000 |
| IEEE 802.1x | ANO |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) | ANO |
| Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication) | ANO |
| Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů | ANO |
| RADIUS CoA | ANO |
| Podpora instance spanning-tree protokolu per VLAN | ANO |
| IEEE 802.1w - Rapid Spanning Tree Protocol | ANO |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | ANO |
| Podpora jumbo rámců (min. 9198 bytes) | ANO |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | ANO |
| Minimální počet HW QoS front | 8 |
| QoS classification – ACL, DSCP, CoS based | ANO |
| QoS marking - DSCP, CoS | ANO |
| QoS - Strict Priority Queue | ANO |
| Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) | ANO |
| QoS Policing | ANO |
| QoS-Hierarchical QoS | ANO, min. 2 úrovně |
| First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP) | ANO |
| IPv6 services (SSH, Syslog) | ANO |
| IPv6 QoS | ANO |
| IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard) | ANO |
| IPv6 Port ACL, VLAN ACL | ANO |
| Možnost definovat povolené MAC adresy na portu | ANO |
| PACL, VACL | ANO |
| IEEE 802.1ae na uplink portech | ANO |
| Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy | ANO |
| Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru | ANO |
| Bezpečnostní funkce umožňující inspekci provozu protokolu ARP | ANO |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | ANO |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | ANO |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, hodnota TTL, ICMP kód, IGMP type | ANO |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | ANO |
| SSHv2 | ANO |
| CLI rozhraní | ANO |
| SNMPv2/v3 | ANO |
| Podpora network boot (iPXE) | ANO |
| Inventarizovatelnost komponent integrovanou RFID identifikací | ANO |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | ANO |
| Záruka a servisní podpora výrobce min. 60 měsíců, výměna či odeslání náhradního zařízení následující pracovní den | Záruka a servisní podpora výrobce min. 60 měsíců, výměna či odeslání náhradního zařízení následující pracovní den |
| Příslušenství | 2x Modul SFP1000-BASE-LX kompatibilních s přepínačem  2x optický patch kabel 1m |

## K3 – patrový přepínač 8p PoE s příslušenstvím (domov mládeže)

|  |  |
| --- | --- |
| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění požadované minimální funkcionality/vlastnosti** |
| Typ přepínače | L2/L3 přepínač |
| Formát přepínače | Fixní konfigurace |
| Bezventilátorový (z důvodu instalace mimo technologické místnosti) | ANO |
| Počet portů 10/100/1000 Base-TX s PoE+ napájením | 8 |
| Minimální PoE budget | 240W |
| Uplink porty | 2x10/100/1000 + 2x10GE SFP+ |
| Min. velikost sdíleného systémového bufferu | 6MB |
| Velikost MAC address tabulky | 32000 |
| Min. počet konfigurovatelných security ACL | 1500 |
| IEEE 802.3ad (Link Aggregation) | ANO |
| IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis | ANO |
| Minimálně 8 linek jako součást Link Aggregation Group trunku | ANO |
| IEEE 802.1Q | ANO |
| Minimální počet aktivních VLAN | 512 |
| IEEE 802.1x | ANO |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) | ANO |
| Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication) | ANO |
| Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů | ANO |
| RADIUS CoA | ANO |
| Podpora instance spanning-tree protokolu per VLAN | ANO |
| IEEE 802.1w - Rapid Spanning Tree Protocol | ANO |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | ANO |
| Podpora jumbo rámců (min. 9198 bytes) | ANO |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | ANO |
| IGMPv2, IGMPv3 | ANO |
| IGMP snooping | ANO |
| MLD snooping | ANO |
| DHCP relay | ANO |
| Minimální počet HW QoS front | 8 |
| QoS classification – ACL, DSCP, CoS based | ANO |
| QoS marking - DSCP, CoS | ANO |
| QoS - Strict Priority Queue | ANO |
| Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) | ANO |
| QoS Policing | ANO |
| QoS-Hierarchical QoS | ANO, min. 2 úrovně |
| IPv6 services (Telnet, SSH, Syslog, DHCP) | ANO |
| IPv6 QoS | ANO |
| IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard) | ANO |
| IPv6 Port ACL, VLAN ACL | ANO |
| Možnost definovat povolené MAC adresy na portu | ANO |
| PACL, VACL | ANO |
| Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny | ANO, případně povýšením firmware |
| IEEE 802.1ae na uplink portech | ANO |
| IEEE 802.1ae (AES-GCM-256) na uplink portech | ANO |
| Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy | ANO |
| Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru | ANO |
| Bezpečnostní funkce umožňující inspekci provozu protokolu ARP | ANO |
| Klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Scalable-Group Tag eXchange Protocol dle RFC draft-smith-kandula-sxp-10 nebo funkčně ekvivalentní). | ANO |
| IEEE 802.3af | ANO |
| IEEE 802.3at | ANO |
| Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače | ANO |
| Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení | ANO |
| IEEE 802.3az | ANO |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | ANO |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | ANO |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, hodnota TTL, ICMP kód, IGMP type | ANO |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | ANO |
| SSHv2 | ANO |
| CLI rozhraní | ANO |
| SNMPv2/v3 | ANO |
| Podpora network boot (iPXE) | ANO |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | ANO |
| Záruka a servisní podpora výrobce min. 60 měsíců, výměna či odeslání náhradního zařízení následující pracovní den | Záruka a servisní podpora výrobce min. 60 měsíců, výměna či odeslání náhradního zařízení následující pracovní den |
| Příslušenství | 2x Modul SFP+ BASE-LX kompatibilních s přepínačem,  2x optický patch kabel 1m |

## K4 – pavilonový přepínač s příslušenstvím (vychovatelé/domov mládeže)

|  |  |
| --- | --- |
| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění požadované minimální funkcionality/vlastnosti** |
| Typ přepínače | L2/L3 přepínač |
| Formát přepínače | Stohovatelný |
| Počet portů 10/100/1000 Base-TX | 48 |
| Uplink porty | 4x1GE SFP |
| Min. velikost sdíleného systémového bufferu | 6MB |
| Velikost MAC address tabulky | 16000 |
| IEEE 802.3ad (Link Aggregation) | ANO |
| IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis | ANO |
| Minimálně 8 linek jako součást Link Aggregation Group trunku | ANO |
| Minimální počet konfigurovatelných Link Aggregation Group trunků | 48 |
| IEEE 802.1Q | ANO |
| Minimální počet aktivních VLAN | 1000 |
| IEEE 802.1x | ANO |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) | ANO |
| Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication) | ANO |
| Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů | ANO |
| RADIUS CoA | ANO |
| Podpora instance spanning-tree protokolu per VLAN | ANO |
| IEEE 802.1w - Rapid Spanning Tree Protocol | ANO |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | ANO |
| Podpora jumbo rámců (min. 9198 bytes) | ANO |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | ANO |
| Minimální počet HW QoS front | 8 |
| QoS classification – ACL, DSCP, CoS based | ANO |
| QoS marking - DSCP, CoS | ANO |
| QoS - Strict Priority Queue | ANO |
| Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) | ANO |
| QoS Policing | ANO |
| QoS-Hierarchical QoS | ANO, min. 2 úrovně |
| First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP) | ANO |
| IPv6 services (SSH, Syslog) | ANO |
| IPv6 QoS | ANO |
| IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard) | ANO |
| IPv6 Port ACL, VLAN ACL | ANO |
| Možnost definovat povolené MAC adresy na portu | ANO |
| PACL, VACL | ANO |
| IEEE 802.1ae na uplink portech | ANO |
| Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy | ANO |
| Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru | ANO |
| Bezpečnostní funkce umožňující inspekci provozu protokolu ARP | ANO |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | ANO |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | ANO |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, hodnota TTL, ICMP kód, IGMP type | ANO |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | ANO |
| SSHv2 | ANO |
| CLI rozhraní | ANO |
| SNMPv2/v3 | ANO |
| Podpora network boot (iPXE) | ANO |
| Inventarizovatelnost komponent integrovanou RFID identifikací | ANO |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | ANO |
| Záruka a servisní podpora výrobce min. 60 měsíců, výměna či odeslání náhradního zařízení následující pracovní den | Záruka a servisní podpora výrobce min. 60 měsíců, výměna či odeslání náhradního zařízení následující pracovní den |
| Příslušenství | 2x Modul SFP1000-BASE-LX kompatibilních s přepínačem,  2x optický patch kabel 1m |

## K5 - pavilonový přepínač s příslušenstvím (domov mládeže)

Každá sada zahrnuje 2ks přepínačů konfigurovaných do jednoho redundantního stohu. Celkem jsou požadovány 2 stohy čili 4 kusy přepínačů.

|  |  |
| --- | --- |
| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění požadované minimální funkcionality/vlastnosti** |
| Typ přepínače | L2/L3 přepínač |
| Formát přepínače | Stohovatelný |
| Stohování požadováno | ANO |
| Počet dedikovaných stohovacích portů | 2 |
| Minimální počet zařízení ve stohu | 8 |
| Minimální kapacita sběrnice stohu | 1 000 Gb/s |
| Sdílení výkonu napájecích zdrojů napříč celým stohem | ANO |
| Stateful Switch Over v rámci stohu | ANO |
| Non-stop Forwarding | ANO (řešení je možné i povýšením firmware) |
| Možnost instalovat interní redundantní napájecí zdroj | ANO |
| Možnost povyšovat uplink modul | ANO |
| Redundantní ventilátory, včetně možnosti jejich výměny za chodu zařízení | ANO |
| Interní redundantní napájecí zdroj požadován | ANO |
| Datový stohovací kabel požadován | ANO |
| Napájecí stohovací kabel součástí dodávky | ANO |
| Počet portů s rychlostí 10/25 Gbps pro výměnný optický modul SFP+/SFP28 | 24 |
| Možnost instalovat rozšiřující modul (uplink) | 8x 1/10/25GE SFP28 |
| Min. velikost sdíleného systémového bufferu | 32MB |
| Velikost MAC address tabulky | 30000 |
| Min. počet IPv4 routes | 600 |
| Min. počet IPv6 routes | 300 |
| Min. počet konfigurovatelných security ACL | 5000 |
| IEEE 802.3ad (Link Aggregation) | ANO |
| IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis | ANO |
| Minimálně 8 linek jako součást Link Aggregation Group trunku | ANO |
| Minimální počet konfigurovatelných Link Aggregation Group trunků | 128 |
| IEEE 802.1Q | ANO |
| Minimální počet aktivních VLAN | 1000 |
| IEEE 802.1x | ANO |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) | ANO |
| Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication) | ANO |
| Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů | ANO |
| RADIUS CoA | ANO |
| Podpora instance spanning-tree protokolu per VLAN | ANO |
| IEEE 802.1w - Rapid Spanning Tree Protocol | ANO |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | ANO |
| Podpora jumbo rámců (min. 9198 bytes) | ANO |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | ANO |
| Směrování protokolů IPv4 a IPv6 v hardware | ANO |
| OSPFv2 | ANO |
| OSPFv3 | ANO |
| IGMPv2, IGMPv3 | ANO |
| IGMP snooping | ANO |
| MLD snooping | ANO |
| DHCP relay | ANO (řešení je možné i povýšením firmware) |
| Minimální počet HW QoS front | 8 |
| QoS classification – ACL, DSCP, CoS based | ANO |
| QoS marking - DSCP, CoS | ANO |
| QoS - Strict Priority Queue | ANO |
| Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) | ANO |
| QoS Policing | ANO |
| QoS-Per Flow policing | ANO |
| QoS-Hierarchical QoS | ANO, min. 2 úrovně |
| First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP) | ANO |
| IPv6 services (Telnet, SSH, Syslog, DHCP) | ANO |
| IPv6 QoS | ANO |
| IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard) | ANO |
| IPv6 Port ACL, VLAN ACL | ANO |
| Možnost definovat povolené MAC adresy na portu | ANO |
| PACL, VACL | ANO |
| Packetové filtry (ACL) podle doménových jmen | ANO |
| IEEE 802.1ae na všech portech | ANO |
| Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy | ANO |
| Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru | ANO |
| Bezpečnostní funkce umožňující inspekci provozu protokolu ARP | ANO |
| Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů | ANO |
| HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů | ANO |
| Podpora SUDI (IEEE 802.1AR) autentizace | ANO |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | ANO |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | ANO |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, hodnota TTL, ICMP kód, IGMP type | ANO |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | ANO |
| SSHv2 | ANO |
| CLI rozhraní | ANO |
| Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu | ANO |
| Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG | ANO |
| Python scripting | ANO |
| Linux shell | ANO |
| Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení | ANO |
| Streaming telemetrie prostřednictvím NETCONF/XML | ANO |
| SNMPv2/v3 | ANO |
| Podpora network boot (iPXE) pres IPv4 i IPv6 | ANO |
| Inventarizovatelnost komponent integrovanou RFID identifikací | ANO |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | ANO |
| NTPv3 server | ANO |
| Záruka a servisní podpora výrobce min. 60 měsíců, výměna či odeslání náhradního zařízení následující pracovní den | Záruka a servisní podpora výrobce min. 60 měsíců, výměna či odeslání náhradního zařízení následující pracovní den |
| Příslušenství | 24x Modul SFP+/SFP28 BASE-LX kompatibilních s přepínačem,  24x optický patch kabel 1m |

## K6 – optický páteřní přepínač s redundantním zdrojem a příslušenstvím

|  |  |
| --- | --- |
| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění požadované minimální funkcionality/vlastnosti** |
| Typ přepínače | L2/L3 přepínač |
| Formát přepínače | Stohovatelný |
| Stohování požadováno | ANO |
| Počet dedikovaných stohovacích portů | 2 |
| Minimální počet zařízení ve stohu | 8 |
| Minimální kapacita sběrnice stohu | 1000 Gb/s |
| Sdílení výkonu napájecích zdrojů napříč celým stohem | ANO |
| Stateful Switch Over v rámci stohu | ANO |
| Non-stop Forwarding | ANO |
| Možnost instalovat interní redundantní napájecí zdroj | ANO |
| Možnost povyšovat uplink modul | ANO |
| Redundantní ventilátory | ANO |
| Redundantní ventilátory vyměnitelné za chodu zařízení | ANO |
| Interní redundantní napájecí zdroj požadován | ANO |
| Datový stohovací kabel požadován | ANO |
| Napájecí stohovací kabel požadován | ANO |
| Počet portů s rychlostí 10/25 Gbit/s pro výměnný optický modul SFP+/SFP28 | 12 |
| Modulární rozšiřující modul (uplink) | 8x 1/10/25GE SFP28 |
| Min. velikost sdíleného systémového bufferu | 16MB |
| Velikost MAC address tabulky | 30000 |
| Min. počet IPv4 routes | 600 |
| Min. počet IPv6 routes | 300 |
| Min. počet konfigurovatelných security ACL | 5000 |
| IEEE 802.3ad (Link Aggregation) | ANO |
| IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis | ANO |
| Minimálně 8 linek jako součást Link Aggregation Group trunku | ANO |
| Minimální počet konfigurovatelných Link Aggregation Group trunků | 128 |
| IEEE 802.1Q | ANO |
| Minimální počet aktivních VLAN | 1000 |
| IEEE 802.1x | ANO |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) | ANO |
| Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication) | ANO |
| Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů | ANO |
| RADIUS CoA | ANO |
| Podpora instance spanning-tree protokolu per VLAN | ANO |
| IEEE 802.1w - Rapid Spanning Tree Protocol | ANO |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | ANO |
| Podpora jumbo rámců (min. 9198 bytes) | ANO |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | ANO |
| Směrování protokolů IPv4 a IPv6 v hardware | ANO |
| OSPFv2 | ANO |
| OSPFv3 | ANO |
| EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868) | ANO |
| ISIS | ANO |
| Směrování dle škálovatelné adresace, dle vícero adresních prostorů (např. Locator/Identifier Separation Protocol (LISP) dle RFC 6830 nebo funkčně ekvivalentní) | ANO |
| BGPv4 | ANO |
| VXLAN s BGP EVPN | ANO |
| Policy based routing uvnitř VRF | ANO |
| Graceful Insertion and Removal | ANO |
| IP Multicast (PIM SSM, PIM SM) | ANO |
| Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF) | ANO |
| MPLS VPN | ANO |
| MPLS VPN přes GRE tunely | ANO |
| MPLS VPN - 6VPE | ANO |
| VXLAN enkapsulace | ANO |
| First Hop Redundancy Protokol (např. VRRP, HSRP) | ANO |
| Reverse path check (uRPF) pro IPv4 i IPv6 | ANO |
| IGMPv2, IGMPv3 | ANO |
| IGMP snooping | ANO |
| MLD snooping | ANO |
| DHCP relay | ANO |
| Minimální počet HW QoS front | 8 |
| QoS classification – ACL, DSCP, CoS based | ANO |
| QoS marking - DSCP, CoS | ANO |
| QoS - Strict Priority Queue | ANO |
| Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) | ANO |
| QoS Policing | ANO |
| QoS-Per Flow policing | ANO |
| QoS-Hierarchical QoS | ANO, min. 2 úrovně |
| First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP) | ANO |
| IPv6 services (Telnet, SSH, Syslog, DHCP) | ANO |
| IPv6 QoS | ANO |
| IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard) | ANO |
| IPv6 Port ACL, VLAN ACL | ANO |
| Možnost definovat povolené MAC adresy na portu | ANO |
| PACL, VACL | ANO |
| Paketové filtry (ACL) podle doménových jmen | ANO |
| Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny | ANO |
| IEEE 802.1ae na všech portech | ANO |
| IEEE 802.1ae (AES-GCM-256) na všech portech | ANO |
| IPSec enkryptace v hardware | ANO |
| IKEv2 | ANO |
| Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy | ANO |
| Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru | ANO |
| Bezpečnostní funkce umožňující inspekci provozu protokolu ARP | ANO |
| Klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Scalable-Group Tag eXchange Protocol dle RFC draft-smith-kandula-sxp-10 nebo funkčně ekvivalentní). | ANO |
| Hardwarová filtrace (access list) podle bezpečnostních rolí uživatelů propagovaných sítí přistupujících k různým skupinám síťových prostředků (např. SGACL, role-based ACL nebo funkčně ekvivalentní) | ANO |
| Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů | ANO |
| HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů | ANO |
| Podpora SUDI (IEEE 802.1AR) autentizace | ANO |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | ANO |
| Multicast DNS (mDNS) gateway | ANO |
| Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur) | ANO |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | ANO |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, hodnota TTL, ICMP kód, IGMP type | ANO |
| Application Visibility – Schopnost detekce bezpečnostních hrozeb v šifrovaném provozu, např. v HTTPS | ANO |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | ANO |
| SSHv2 | ANO |
| CLI rozhraní | ANO |
| Aplikace softwarových záplat, nikoli povyšování celého firmware | ANO |
| SNMPv2/v3 | ANO |
| Podpora network boot (iPXE) pres IPv4 i IPv6 | ANO |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | ANO |
| Vzdálený port mirroring (ERSPAN) | ANO |
| NTPv3 server | ANO |
| Záruka a servisní podpora výrobce min. 60 měsíců, výměna či odeslání náhradního zařízení následující pracovní den | Záruka a servisní podpora výrobce min. 60 měsíců, výměna či odeslání náhradního zařízení následující pracovní den |
| Příslušenství | 12x Modul SFP+/SFP28 BASE-LR  12x optický patch kabel 1m  1× stohovací kabel |

## K7 – přepínač 24p PoE s příslušenstvím pro wifi

|  |  |
| --- | --- |
| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění požadované minimální funkcionality/vlastnosti** |
| Typ přepínače | L2/L3 přepínač |
| Formát přepínače | Stohovatelný |
| Redundantní ventilátory | ANO |
| Minimální PoE budget | 370W |
| Počet portů 10/100/1000 Base-TX s PoE+ napájením | 24 |
| Uplink porty | 4x10GE SFP+ |
| Min. velikost sdíleného systémového bufferu | 6MB |
| Velikost MAC address tabulky | 16000 |
| Min. počet IPv4 routes | 3000 |
| Min. počet IPv6 routes | 1500 |
| Min. počet konfigurovatelných security ACL | 1000 |
| IEEE 802.3ad (Link Aggregation) | ANO |
| IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis | ANO |
| Minimálně 8 linek jako součást Link Aggregation Group trunku | ANO |
| Minimální počet konfigurovatelných Link Aggregation Group trunků | 24 |
| IEEE 802.1Q | ANO |
| Minimální počet aktivních VLAN | 1000 |
| IEEE 802.1x | ANO |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) | ANO |
| Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication) | ANO |
| Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů | ANO |
| RADIUS CoA | ANO |
| Podpora instance spanning-tree protokolu per VLAN | ANO |
| IEEE 802.1w - Rapid Spanning Tree Protocol | ANO |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | ANO |
| Podpora jumbo rámců (min. 9198 bytes) | ANO |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | ANO |
| IGMPv2, IGMPv3 | ANO |
| IGMP snooping | ANO |
| MLD snooping | ANO |
| DHCP relay | ANO |
| Minimální počet HW QoS front | 8 |
| QoS classification – ACL, DSCP, CoS based | ANO |
| QoS marking - DSCP, CoS | ANO |
| QoS - Strict Priority Queue | ANO |
| Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) | ANO |
| QoS Policing | ANO |
| QoS-Hierarchical QoS | ANO, min. 2 úrovně |
| First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP) | ANO |
| IPv6 services (SSH, Syslog) | ANO |
| IPv6 QoS | ANO |
| IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard) | ANO |
| IPv6 Port ACL, VLAN ACL | ANO |
| Možnost definovat povolené MAC adresy na portu | ANO |
| PACL, VACL | ANO |
| IEEE 802.1ae na uplink portech | ANO |
| Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy | ANO |
| Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru | ANO |
| Bezpečnostní funkce umožňující inspekci provozu protokolu ARP | ANO |
| Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače | ANO |
| Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení | ANO |
| IEEE 802.3az | ANO |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | ANO |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | ANO |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, hodnota TTL, ICMP kód, IGMP type | ANO |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | ANO |
| SSHv2 | ANO |
| CLI rozhraní | ANO |
| SNMPv2/v3 | ANO |
| Podpora network boot (iPXE) | ANO |
| Inventarizovatelnost komponent integrovanou RFID identifikací | ANO |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | ANO |
| NTPv3 server | ANO |
| Záruka a servisní podpora výrobce min. 60 měsíců, výměna či odeslání náhradního zařízení následující pracovní den | Záruka a servisní podpora výrobce min. 60 měsíců, výměna či odeslání náhradního zařízení následující pracovní den |
| Příslušenství | 2x Modul SFP+ BASE-LX kompatibilních s přepínačem  2x optický patch kabel 1m |

## K8 – přepínač 12p PoE s příslušenstvím pro wifi

|  |  |
| --- | --- |
| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění požadované minimální funkcionality/vlastnosti** |
| Typ přepínače | L2/L3 přepínač |
| Formát přepínače | Fixní konfigurace |
| Bezventilátorový (z důvodu instalace mimo technologické místnosti) | ANO |
| Počet portů 10/100/1000 Base-TX s PoE+ napájením | 12 |
| Minimální PoE budget | 240W |
| Uplink porty | 2x10/100/1000 + 2x10GE SFP+ |
| Min. velikost sdíleného systémového bufferu | 6MB |
| Velikost MAC address tabulky | 32000 |
| Min. počet konfigurovatelných security ACL | 1500 |
| IEEE 802.3ad (Link Aggregation) | ANO |
| IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis | ANO |
| Minimálně 8 linek jako součást Link Aggregation Group trunku | ANO |
| IEEE 802.1Q | ANO |
| Minimální počet aktivních VLAN | 512 |
| IEEE 802.1x | ANO |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) | ANO |
| Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication) | ANO |
| Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů | ANO |
| RADIUS CoA | ANO |
| Podpora instance spanning-tree protokolu per VLAN | ANO |
| IEEE 802.1w - Rapid Spanning Tree Protocol | ANO |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | ANO |
| Podpora jumbo rámců (min. 9198 bytes) | ANO |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | ANO |
| IGMPv2, IGMPv3 | ANO |
| IGMP snooping | ANO |
| MLD snooping | ANO |
| DHCP relay | ANO |
| Minimální počet HW QoS front | 8 |
| QoS classification – ACL, DSCP, CoS based | ANO |
| QoS marking - DSCP, CoS | ANO |
| QoS - Strict Priority Queue | ANO |
| Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) | ANO |
| QoS Policing | ANO |
| QoS-Hierarchical QoS | ANO, min. 2 úrovně |
| IPv6 services (Telnet, SSH, Syslog, DHCP) | ANO |
| IPv6 QoS | ANO |
| IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard) | ANO |
| IPv6 Port ACL, VLAN ACL | ANO |
| Možnost definovat povolené MAC adresy na portu | ANO |
| PACL, VACL | ANO |
| Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny | ANO, povýšením firmware |
| IEEE 802.1ae na uplink portech | ANO |
| IEEE 802.1ae (AES-GCM-256) na uplink portech | ANO |
| Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy | ANO |
| Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru | ANO |
| Bezpečnostní funkce umožňující inspekci provozu protokolu ARP | ANO |
| Klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Scalable-Group Tag eXchange Protocol dle RFC draft-smith-kandula-sxp-10 nebo funkčně ekvivalentní). | ANO |
| IEEE 802.3af | ANO |
| IEEE 802.3at | ANO |
| Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače | ANO |
| Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení | ANO |
| IEEE 802.3az | ANO |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | ANO |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | ANO |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, hodnota TTL, ICMP kód, IGMP type | ANO |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | ANO |
| SSHv2 | ANO |
| CLI rozhraní | ANO |
| SNMPv2/v3 | ANO |
| Podpora network boot (iPXE) | ANO |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | ANO |
| Záruka a servisní podpora výrobce min. 60 měsíců, výměna či odeslání náhradního zařízení následující pracovní den | Záruka a servisní podpora výrobce min. 60 měsíců, výměna či odeslání náhradního zařízení následující pracovní den |
| Příslušenství | 2x Modul SFP+ BASE-LX kompatibilních s přepínačem  2x optický patch kabel 1m |

## K9 – licence SW pro řízení přístupu do sítě 802.1x

Vzhledem k tomu, že Zadavatel v současnosti používá systém 802.1x společnosti Cisco, Identity service engine, který byl pořízen v rámci dotačního projektu IROP a stále je v režimu udržitelnosti, není možné jej nahradit. Zároveň Zadavatel požaduje i v částech prostředí, které pokrývá tento projekt, využití jednotného systému pro řízení přístupu do sítě.

V rámci dodávky je tudíž požadováno dodání licencí:

**300ks ISE-A-LIC (Cisco Identity Service Engine Advantage) včetně technické podpory výrobce na 5 let.**

Řešení 802.1x musí dále využívat prostředky stávajícího RADIUS serveru EduRoam a dále umožnit užití autentizačních prostředků pro přístup do sítě z nově budované MS Active Directory.

## K10 – WiFi přístupový bod s příslušenstvím

AP typ 1

| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění požadované minimální funkcionality/vlastnosti** |
| --- | --- |
| ***WiFi Access Point*** | ***2 kusy*** |
| Access Point určený pro instalaci na strop/podhled | PODPORUJE |
| Typ antén | Integrované pro obě pásma |
| Dvě rádia pracující v režimu 2,4 a 5 GHz pro standardní prostředí nebo duální 5 GHz pro HD nasazení, možnost statické i dynamické volby režimu | PODPORUJE |
| Samostatné rádio pro monitorování 2,4 a 5 GHz RF spektra – detailní spektrální analýza, detekce útoků na bezdrátovou sít, lokalizace klientů | PODPORUJE |
| Podpora standardů 802.11a/b/g/n/ac a Wi-Fi6 (802.11ax) | PODPORUJE |
| Podpora minimálně 4x4 MIMO, MU-MIMO, UL/DL OFDMA, TWT, BSS Coloring a až 160 MHz kanál pro 802.11ax | PODPORUJE |
| Minimální počet inzerovaných SSID (BSSID) per radio | 8 |
| Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu směrem k 802.11 n/ac/ax klientům (Tx Beam Forming) | PODPORUJE |
| Podpora mechanismu pro přepojení klientů z 2,4GHz do 5GHz pásma | PODPORUJE |
| Access Pointy obsahují X.509 certifikát s lokální platností pro nasazeni PKI | PODPORUJE |
| Podpora autentizace Access Pointu do LAN sítě pomocí 802.1x, AP obsahují 802.1x supplikant | PODPORUJE |
| Podpora detekce a monitorování problémů WLAN odchytáváním provozu na AP a jeho zasíláním do Ethernetového analyzátoru (např. Wireshark) | PODPORUJE |
| Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a přes IPv4 pomocí Telnet a SSH | PODPORUJE |
| Hardwarová podpora spektrální analýzy s podporou 160 MHz kanálů (detekce zdroje rušivého signálu – interference) | PODPORUJE |
| Podpora rozpoznání zdroje rušivého signálu podle signatur | PODPORUJE |
| Access Point obsahuje radio podporující BLE 5.0, ZigBee, Thread a USB 2.0 port | PODPORUJE |
| 1 x 100/1000/2500 Mbit/s RJ45 ethernet rozhraní kompatibilní  s 802.3bz | PODPORUJE |
| Možnost 802.3af/at PoE napájení AP z přepínače nebo injectoru – plná funkce AP při použití 802.3at, v případě 802.3af AP běží minimálně v režimu 1x1 MIMO pro obě rádiová pásma bez sníženého vysílacího výkonu | PODPORUJE |
| AP uzavřené konstrukce bez větracích otvorů a ventilátoru | PODPORUJE |
| Součástí AP je plechový úchyt pro instalaci na strop nebo stěnu | PODPORUJE |
| AP je fyzicky zabezpečitelné/zamknutelné k okolním pevným částem. | PODPORUJE |
| Důvěryhodný HW/SW – AP používá bezpečný zavaděč OS, ověřování podpisu OS, kontrolu autentičnosti HW a mechanizmy pro ochranu SW a HW proti útokům | PODPORUJE |
| Součástí dodávky každého ze dvou dodávaných AP tohoto typu jsou licence pro kontrolér bezdrátové sítě minimálně na dobu pěti let, který poběží ve virtualizovaném prostředí, viz. specifikace kontroleru níže  Součástí dodávky každého AP jsou licence přístup AP ke kontroléru bezdrátové sítě minimálně na dobu 5 let, pokud je pro dodané řešení taková licence potřeba | OBSAHUJE |
| Plná podpora AP na dodávaném kontroléru | PODPORUJE |
| Záruka | Záruka a podpora výrobce min. 60 měsíců |

AP typ 2

| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění požadované funkcionality/vlastnosti** |
| --- | --- |
| ***WiFi Access Point*** | ***71 kusů*** |
| Access Point určený pro instalaci na strop/podhled | PODPORUJE |
| Typ antén | Integrované pro obě pásma |
| Access Point vybavený radiem pro 2,4 a 5 GHz pásmo, podpora standardu 802.11a/b/g/n/ac a Wi-Fi6 (802.11ax) | PODPORUJE |
| Podpora minimálně 4x4 MIMO, MU-MIMO, UL/DL OFDMA, TWT, BSS Coloring a až 160 MHz kanál pro 802.11ax | PODPORUJE |
| Minimální počet inzerovaných SSID (BSSID) per radio | 8 |
| Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu směrem k 802.11 n/ac/ax klientům (Tx Beam Forming) | PODPORUJE |
| Podpora mechanismu pro přepojení klientů z 2,4GHz do 5GHz pásma | PODPORUJE |
| Access Pointy obsahují X.509 certifikát s lokální platností pro nasazeni PKI | PODPORUJE |
| Podpora autentizace Access Pointu do LAN sítě pomocí 802.1x, AP obsahují 802.1x supplikant | PODPORUJE |
| Podpora detekce a monitorování problémů WLAN odchytáváním provozu na AP a jeho zasíláním do Ethernetového analyzátoru (např. Wireshark) | PODPORUJE |
| Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a přes IPv4 pomocí Telnet a SSH | PODPORUJE |
| Access Point obsahuje Bluetooth low-energy (BLE) 5.0 rádio a USB 2.0 port | PODPORUJE |
| 1 x 100/1000/2500 Mbit/s RJ45 ethernet rozhraní kompatibilní  s 802.3bz | PODPORUJE |
| Možnost 802.3af/at PoE napájení AP z přepínače nebo injectoru, v případě použití 802.3af AP běží minimálně v režimu 2x2 MIMO pro obě rádiová pásma bez sníženého vysílacího výkonu | PODPORUJE |
| AP uzavřené konstrukce bez větracích otvorů a ventilátoru | PODPORUJE |
| Součástí AP je plechový úchyt pro instalaci na strop nebo stěnu | PODPORUJE |
| AP je fyzicky zabezpečitelné/zamknutelné k okolním pevným částem. | PODPORUJE |
| Důvěryhodný HW/SW – AP používá bezpečný zavaděč OS, ověřování podpisu OS, kontrolu autentičnosti HW a mechanizmy pro ochranu SW a HW proti útokům | PODPORUJE |
| Součástí dodávky každého AP jsou licence přístup AP ke kontroléru bezdrátové sítě minimálně na dobu 5 let, pokud je pro dodané řešení taková licence potřeba | OBSAHUJE |
| Plná podpora AP na dodávaném kontroléru | PODPORUJE |
| Záruka | Záruka a podpora výrobce min. 60 měsíců |

**Kontrolér bezdrátové sítě**

|  |  |
| --- | --- |
| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění požadované minimální funkcionality/vlastnosti** |
| Požadovaný formát zařízení | Virtuální appliance kompatibilní s virtualizačním prostředím Zadavatele |
| Minimální podporovaná propustnost pro centrálně přepínaná data | 5 Gb/s |
| Licence dle počtu nově pořizovaných AP, možnost upgradu až na minimálně 1000 a více registrovaných AP | PODPORUJE |
| Podpora stávajících AP řady 1700/2700/18xx/2800, které má Zadavatel nasazeny ve své infrastruktuře, a nově pořizovaných AP | PODPORUJE |
| Minimální počet současně připojených klientů | 64000 |
| Redundance na úrovni kontrolérů a jejich portů, výpadek aktivního kontroléru v redundantním páru nemá žádný dopad na provoz již připojených klientů (tj. bez potřeby reautentizace) | PODPORUJE |
| Upgrade kontrolerů bez výpadku připojených klientů | PODPORUJE |
| Možnost postupného upgradu nově pořizovaných i stávajícího kontroleru a všech AP Zadavatele z důvodu zkrácení doby výpadku | PODPORUJE |
| Lokální síť - možnost tunelování uživatelských dat z AP až na kontroler, možnost šifrování těchto uživatelských dat bez výrazného vlivu na propustnost | PODPORUJE |
| Mesh síť - podpora mesh sítí, současné připojení normálních a mesh AP k jednomu kontroléru | PODPORUJE |
| Vzdálené lokality - možnost lokálního bridgování uživatelských dat per SSID přímo na příslušném AP | PODPORUJE |
| Šifrovaná řídící komunikace AP-kontroler | PODPORUJE |
| Současná funkčnost AP pro přenos dat, analýzu spektra a detekci bezpečnostních incidentů | PODPORUJE |
| Bezpečnost a Guest Access |  |
| Podpora 802.11i, respektive jeho implementace WPA2 včetně enterprise variant autentizace/šifrování | PODPORUJE |
| Podpora WPA3 – WPA3 Enterprise, WPA3 SAE, WPA3 OWE | PODPORUJE |
| PSK autentizace vč. možnosti různých PSK klíčů pro různé klienty v rámci jednoho SSID | PODPORUJE |
| Podpora standardu „802.11w“ pro ochranu řídících rámců na AP a klientovi | PODPORUJE |
| Podpora standardu „802.11u“ pro výběr SSID a autentizaci klienta | PODPORUJE |
| Integrované řešení návštěvnického přístupu s možností webové autentizace (včetně nativních IPv6 klientů), bezpečné oddělení od zaměstnaneckého provozu, funkční i v módu lokálního bridgování uživatelských dat přímo na AP | PODPORUJE |
| Podpora řešení návštěvnického přístupu pro klienty bezdrátové i drátové sítě | PODPORUJE |
| Možnost omezit počet klientů per SSID | PODPORUJE |
| Lokální profilování zařízení – per uživatel a per zařízení | PODPORUJE |
| Integrovaný IDS systém pro detekci cizích AP (Rogue AP) a klientů v AdHoc režimu, možnost vynuceného odpojení klientů od cizích AP | PODPORUJE |
| Podpora Flexible NetFlow a exportu záznamů (dle RFC 3954) o datových tocích uživatelů (vč. zdrojové a cílové IP adresy, portů, WLAN ID, počtu paketů a objemu přenesených dat) směrem k externímu kolektoru | PODPORUJE |
| Podpora pro analýzu šifrovaného provozu | PODPORUJE |
| Podpora integrace pro ochranu protokolu DNS | PODPORUJE |
| **Rychlý roaming** |  |
| Automatizované řešení roamingu uživatelů v rámci AP připojených na nově pořizovaný i stávající kontroler Zadavatele | PODPORUJE |
| Podpora standardu „802.11r“ pro rychlý roaming klientů mezi AP, možnost selektivního využití 802.11r na sdíleném SSID pouze pro zařízení, které tento standard podporují | PODPORUJE |
| Podpora standardu „802.11k“ pro optimalizaci roamingu | PODPORUJE |
| Podpora standardu „802.11v“ pro optimalizaci připojení klienta | PODPORUJE |
| **QoS a řízení provozu v bezdrátové síti** |  |
| Podpora 802.11e/WMM | PODPORUJE |
| Diferenciace úrovní QoS pro různé služby a skupiny uživatelů (zaměstnance a návštěvníky), možnost obousměrného omezení propustnosti per klient. | PODPORUJE |
| Mechanismy řízení přístupu (Call Admission Control) pro hlasový i video provoz. Konfigurovatelné parametry max. zátěže a šířky pásma. | PODPORUJE |
| Podpora Video-streamingu se spolehlivým multicastem | PODPORUJE |
| Optimalizace multicast provozu v bezdrátové síti (IGMP snooping) | PODPORUJE |
| **Správa frekvenčního pásma, konfigurační profily** |  |
| Aplikační inspekce přenášeného provozu (DPI na 7. vrstvě ISO/OSI na základě aplikačních signatur) umožňující rozpoznání jednotlivých aplikací, grafické zobrazení statistik a možnost řízení QoS per rozpoznaná aplikace | PODPORUJE |
| Automatizovaná centrální správa frekvenčního pásma | PODPORUJE |
| Monitoring rádiového spektra vč. 20/40/80/160 MHz kanálů, možnost okamžité automatické centralizovaně řízené reakce (změna kanálu nebo jeho šířky, změna vysílacího výkonu), grafické vyobrazení informací o kvalitě signálu | PODPORUJE |
| Automatické zvýšení vysílacího výkonu okolních AP při výpadku AP („self healing“) | PODPORUJE |
| Automatické přepínání rádií mezi 2,4 a 5 GHz jednotlivých AP | PODPORUJE |
| Možnost detekce rušivých signálů (interference) a identifikace zdrojů interference na základě signatur | PODPORUJE |
| Mesh síť – automatický výběr vhodného kanálu pro backhaul, automatické sestavení optimálního mesh stromu, monitorování všech kanálů na pozadí s rychlou konvergencí v případě výpadku primárního nadřazeného AP | PODPORUJE |
| Troubleshooting radiového signálu a automatické řešení problému rušivého signálu, generování alarmů na základě překročení prahových hodnot kvality signálu | PODPORUJE |
| Možnost definovat různé konfigurační profily a ty následně přiřadit vybraným AP (např. dle umístění AP, bezpečnostních pravidel atd.). | PODPORUJE |
| Možnost vytvořit různé rádiové profily (nastavení kanálů, rychlostí) a ty následně přiřadit vybraným AP. | PODPORUJE |
| **Podpora IPv6** |  |
| Podpora IPv6 – management kontroleru (vč. Syslog, radius) | PODPORUJE |
| Podpora IPv6 – komunikace AP-kontroler | PODPORUJE |
| Podpora IPv6 – Guest Access i pro nativní klienty vč. webové autentizace pro IPv6 klienty | PODPORUJE |
| Podpora IPv6 – IPv6 multicast, MLD snooping | PODPORUJE |
| Podpora IPv6 – bezpečnost (RA Guard, IPv6 Source Guard, DHCPv6 Server Guard, ACL) | PODPORUJE |
| Podpora IPv6 – ND cache na kontroleru, optimalizace přenosu ND zpráv, rate-limiting pro RA | PODPORUJE |
| Centrální administrace správců s granularitou přístupových práv | PODPORUJE |
| Podpora správy přes serial CLI nebo přes IP pomocí SSH/telnet a https web GUI, SNMP | PODPORUJE |
| RJ45 konzolový port a/nebo USB konzolový port, dedikovaný ethernetový RJ45 management port | PODPORUJE |
| Podpora API rozhraní pro plnou konfiguraci kontroleru pomocí NETCONF, RESTCONF za použití YANG data modelů. Podpora exportu provozních dat z kontroleru. | PODPORUJE |
| Možnosti využití vestavěného Python API pro automatizovanou správu | PODPORUJE |
| Důvěryhodný SW – kontroler používá bezpečný zavaděč OS, ověřování podpisu SW komponent, kontrolu autentičnosti a mechanizmy pro ochranu proti útokům | PODPORUJE |

## K11 – licence SW pro řízení přístupových oprávnění – Identity management system

|  |  |
| --- | --- |
| **Parametr** | **Popis povinného parametru** |
| Základní funkce | Identity management system (dále jen jako IDM nebo Systém) bude udržovat a spravovat identity a organizační strukturu organizace – třídy, učitelský sbor, administrativa atd. Spravované identity budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy. Identity budou ukládány v databázi. |
| Licence | Poskytnutá licence umožní nasazení a provoz IDM bez omezení na počet uživatelů, spravovaných identit a napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Zadavatele (počet záznamů, velikost databází atd.).  V případě, že nebude možné nabídnout řešení bez omezení počtu uživatelských licencí, stanový zadavatele minimální požadavek na počet uživatelů ve výši 1900 (z toho 1600 žáci a studenti a 300 zaměstnanci), který však musí umožnit jejich plovoucí užití, tedy po vyřazení studentů posledního ročníku a nástupu nového ročníku licence užít pro nové uživatele. |
| Škálovatelnost | Systém musí umožnit zvyšování výkonu (zlepšování odezvy) rozložením komponent Systému na více serverů – minimálně 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 atd.). |
| Logování | Systém bude poskytovat auditní logy pro pořizovaný logovací a monitorovací systém |
| Logování systému | Systém obsahuje logování min. 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 umožní 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. |
| Parametr hesla | IDM musí umožnit užití a synchronizaci užití stejného hesla pro přístup k IDM a pro stejného uživatele i pro přístup ke službám prostřednictvím MS Active Directory. |
| Požadavky na portál – obecné | IDM bude obsahovat 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 bude umožňovat přehlednou správu samostatných identifikovatelných objektů – referenčních objektů, na které se identity mohou odkazovat: min. 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 bude umožňovat vyhledávat i bez diakritiky (např. zadání Cizova vyhledává i Čížová apod.) |
| Obrázky | Systém umožní k jednotlivým účtům (identitám) přikládat obrázky – fotografie. |
| Ochrana proti chybám | Systém bude obsahovat 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 bude obsahovat přehled uživatelů aktuálně pracujících s Portálem |
| Slučování identit | Systém umožní 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 min. na úrovni organizační jednotky (nebo hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, přiřazení aplikační role, editace identity apod.) |
| Granularita oprávnění | Oprávnění přidělovaná uživatelům a správcům bude možné definovat a přidělovat pro jednotlivé části systému (identity, referenční objekty, notifikací, synchronizací, konfigurace systému, webové služby atd.). U jednotlivých částí bude možnost definovat akce, které může uživatel s přidělenými oprávnění v konkrétní části IDM provádět.  Zadavatel dále požaduje specifickou položku pro uživatele a skupiny uživatelů, a to číslo čipu a jeho kód, který slouží jak přístupový identifikátor a který zadavatel požaduje prostřednictvím IDM zapisovat do MS AD tak, aby mohl být čten dalšími systémy napojenými na MS AD. Je požadována možnost zadání a zápisu tohoto typu položky do AD (zápis, změna, odstranění, logování všech činností). |
| Časová omezení | IDM bude umožňovat přiřazení rolí konkrétní identitě, pracovní pozici, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení platnosti přiřazení. Po vypršení platnosti přiřazení IDM rolí přiřazenému objektu automaticky odebere. |
| Vícenásobné vazby | Možnost přiřazení identit k pracovním pozicím ve vazbě M:N. Identita může být v IDM evidována na více pracovních pozicích současně a současně na pracovní pozici může být evidováno více identit. |
| Přehled rolí | Možnost zobrazení přidělených rolí k jednotlivým identitám s přehledným rozlišením rolí navázaných na pracovní pozici, rolí navázaných na identitu, rolí navázaných na organizační jednotku, rolí navázaných na skupinu a delegovaných role. |
| Přehled dědičností | IDM umožní evidenci a přehledné souhrnné zobrazení všech rolí včetně informace, odkud uživatel roli zdědil (z organizační jednotky, pracovní pozice, skupiny) nebo zda má nějakou roli od někoho delegovánu. |
| Skupiny | IDM bude obsahovat 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 musí být možno provádět pomocí SMS (tj. IDM musí být možné na SMS bránu či službu napojit). Rozhraní musí umožnit i běžnou změnu hesla (bez resetu).  Mimo SMS musí umožnit autentizační proces i možnost užití autentizace službou MS Authenticator, kterou má k dispozici zadavatel jako součást M365. |
| Individualizace | IDM umožní uživatelům individuálně nastavit vlastní zobrazení rozhraní - min. zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku (buď několik přednastavených hodnot nebo možnost ručního nastavení) - vždy pro každý seznam samostatně. |
| Upozornění | IDM zajistí zasílání konfigurovatelných emailových upozornění min. pro následující události: vytvoření a změna identity, referenčního objektu (pracovní pozice, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role atd.), problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu. |
| Včasná upozornění | Upozornění na vypršení časových termínů musí být možno zasílat v předstihu. Velikost předstihu (např. 10 dnů) musí být možno konfigurovat pro každý typ upozornění samostatně. |
| Šablony upozornění | Šablony upozornění umožní definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám musí být možné nastavovat různé příjemce pro různé části organizační struktury (např. odbor, oddělení) apod. Šablony musí umožnit vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu. |
| Kontext upozornění | Pro zasílání jednotlivých typů upozornění bude 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 uvedeny 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 bude možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových souborů jako XML, CSV atd. z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM. |
| Auditní report | IDM umožní export auditního reportu z údajů o identitách uložených v IDM, a to i historických. Auditní reporty budou minimálně ve formátu XML nebo CSV a budou obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IDM, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti. |
| Auditní report – výběr | Identity pro generování auditního reporty musí být 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 musí být exportovatelné 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.  Součástí dodané IDM bude dokumentace rozhraní, kterou bude moci zadavatel užít při pořizování nového systému jako požadavek na jeho integraci. |
| 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 bude možné je zobrazit v prostředí Portálu |
| Služby rozhraní WS | Rozhraní bude poskytovat minimálně 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. 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  - Personální systém PERM3  - Systém Bakaláři  - Docházkový systém  Zajištění konektorů a licencí na straně stávajících informačních systémů (s výjimkou globálních výrobců jako je společnost Microsoft, které jsou veřejně publikované a dostupné) zajišťuje zadavatel a není součástí tohoto plnění. |
| Školský systém | IDM bude napojeno na školský informační systém Bakaláři. Ze systému Bakaláři budou načítány údaje o organizační struktuře, osobách a tyto údaje budou pro IDM sloužit jako zdrojové.  Popis rozhraní systému Bakaláři je obsažen v příloze č. 1 této dokumentace. |
| Personální systém | IDM napojeno na personální systém PERM3. Z personálního systému budou načítány údaje o organizační struktuře, hierarchii pracovních míst, osobách a tyto údaje budou pro IDM sloužit jako zdrojové.  Popis rozhraní systému PERM3 je obsažen v příloze č. 2 této dokumentace. |
| Docházka a strava | Součástí prostředí zadavatele je i dále systém Docházka a strava od Z-Ware.  Tento systém bude integrován na AD, které bude spravováno prostřednictvím IDM.  Zadavatel v rámci implementace předá dodavateli IDM požadavky na konfiguraci AD prostřednictvím IDM, ze které systém této třetí strany bude čerpat.  Dodavatel IDM se zavazuje připravit požadované procesy pro zápis uživatelů, skupin uživatelů a jejich práv dle poskytnuté dokumentace zadavatelem. |
| Integrace na Active Directory | IDM musí obsahovat konektor umožňující napojení na Microsoft Active Directory s následující funkcionalitou:  komplexní správu účtů, kontaktů, certifikátů a skupin (založení, změnu atributů, zrušení, změnu hesla atd.)  založení domovského adresáře včetně nastavení oprávnění - Dodavatel navrhne, které části domovského adresáře uživatele je vhodné mít lokálně a které cloudově (M365 OneDrive) a pro dané nastavení navrhne politiky včetně šablon pro konfiguraci. Pro sdílené soubory a adresáře dodavatel navrhne pravidla a politiky a optimální formu dosažení požadovaného sdílení s užitím lokálních i cloudových služeb.  správu účtů a jejich certifikátů včetně inicializačního načtení z AD  správu skupin a členství ve skupinách včetně inicializačního načtení z AD  správu organizačních jednotek včetně inicializačního načtení z AD |
| Integrace na O365 | Konektor IDM musí umožnit napojení na MS O365 s následující funkcionalitou:  inicializační načtení dat  správa lokálních identit  správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí |
| Podpora software | K dodanému IDM bude uzavřena samostatná smlouva o technické podpoře a rozvoji, která je samostatnou přílohou zadávacích podmínek. |

## K12 – Licence SW ochrany koncových stanic a serverů před škodlivým kódem (ANTI-X)

|  |  |
| --- | --- |
| **Položka** | **Popis minimálního parametru** |
| Základní technické požadavky na anti-X | Licence pro min 670 zařízení |
| **PREVENCE** |
| Pokročilá ochrana před hrozbami. |
| Hlášení událostí do jedné management konsole. |
| Ochrana před útoky, které šifrují MBR. |
| Multiplatformní ochrana proti malwaru pro systémy Windows, Linux i macOS z jedné management konsole. |
| Ochrana i pro starší verze systému Windows. |
| Filtrování webových kategorií (zejména drogy, hazard, zbraně, extrémismus, násilí, sex, zločin, rasismus). |
| Blokování malware i na renomovaných stránkách. |
| Blokování phishingovým webů. |
| Ochrana proti exploitům. |
| Ochrana před útoky využívajícími dosud neznámé zranitelnosti - tzv. nultého dne. |
| Ochrana proti bez souborovým útokům. |
| Ochrana proti síťovým útokům a hrozbám. |
| DLP integrované do koncových bodů bez nutnosti instalace pluginů, s předdefinovanou sadou detekčních pravidel pro běžné typy dat a v případě potřeby možnost vytvořit vlastní pravidla pomocí regulárních výrazů. |
| Pokročilá ochrana pro virtualizovaná prostředí Vmware i Hyper-V. Možnost volby mezi tenkým a plným klientem. |
| Dynamická obrana s automatizovanou ochranou proti aktivním útočníkům a útokům na klávesnici. |
| Sandbox. |
| Strojové učení. |
| Umělá inteligence. |
| Ochrana AV klienta proti odinstalaci nebo změně unikátním heslem, které je odlišné pro každou stanici. |
| **DETEKCE** |
| Pokročilá detekce hrozeb - detekce neznámého malware a potenciálně nežádoucí aplikace. |
| Detekce ransomware na základě jeho chování. |
| Zastavení nových variant a dosud neviděných ransomware útoků. |
| Kontrola aplikací - možnost kontrolovat instalaci, sledovat používání nebo blokovat spouštění aplikací na koncových bodech podle předdefinovaných kategorií. |
| Detekce a analýza hrozeb a anomálií. |
| Detekce hackerských nástrojů. |
| Vyšetřování detekcí řízené umělou inteligencí. |
| Kontrola stavu účtů pro identifikaci odchylek v zabezpečení a upozornění na rizikové chybné konfigurace. |
| Kontrola připojovaných zařízení - možnost vytváření zásad pro blokování jednotek USB, možnost zablokovat jednotlivé značky nebo modely. |
| **REAKCE** |
| Plná funkcionalita pro EDR/XDR. |
| Možnost integrace produktů třetích stran, například s firewallem, jako zdrojů informací pro XDR. |
| Režim uzamknutí serverového OS neumožňující spuštění jakékoliv neschválené aplikace. |
| Automatizované izolování napadeného koncového bodu. |
| Aktivní zmírnění útoků. |
| Automatizované čištění malwaru nebo zablokování hrozby. |
| Zastavení ransomwaru a šifrování souborů a poté automatické vrácení zašifrovaných souborů zpět do bezpečného stavu bez ohledu na velikost nebo typ souboru. |
| Vizualizace incidentu. Upozornění na útok, poskytnutí podrobností o útoku, automatizace reakce pomocí nástroje XDR, možnost požádat o pomoc tým výrobce. |
| Živý terminál pro vyšetřování incidentu. Průvodce vyšetřováním poskytuje návrhy dalších kroků, jako je prozkoumání zvýrazněných procesů a izolace počítače. |
| Možnost vzdáleně přistupovat k zařízením se systémy Windows, Mac a Linux prostřednictvím příkazového řádku a provádět další šetření, instalovat a odinstalovávat software nebo odstraňovat problémy, které nejsou vyřešeny automaticky. |
| Možnost použití příkazového řádku pro provozní činnosti IT, jako je restartování nebo instalace a odinstalace softwaru. |
| Podpora API. |

## K13 – licence pro správu kryptografických prostředků

|  |  |
| --- | --- |
| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění minimálně požadované funkcionality/vlastnosti** |
| SW pro zvýšení ochrany dat pomocí šifrovaní úložišť. | ANO |
| Jedna management konzole. | ANO |
| Šifrování pro koncové body s různými operačními systémy. | ANO |
| Podpora šifrování pro Win11 | ANO |
| Podpora šifrování pro Win10 | ANO |
| Podpora šifrování pro Mac OS X | ANO |
| Správa a audit nástrojů Microsoft BitLocker. | ANO |
| Šifrování dat na lokálním disku. | ANO |
| Šifrování dat na externích médiích včetně samošifrovacích jednotek. | ANO |
| Správa a audit externích médií včetně samošifrovacích jednotek. | ANO |
| Umožňuje úplné zakázání portu USB proti neautorizovanému připojení externí datové jednotky. | ANO |
| Šifrování dat na mobilních zařízeních. | ANO |
| Šifrování dat ve veřejných cloud úložných službách (OneDrive, DropBox, Box). | ANO |
| Šifrování musí být pro koncové uživatele transparentní. (Práce s daty jsou pro autorizovaného a ověřeného uživatele stejné jako před jejich zašifrováním.) | ANO |
| Nasazení šifrování je bez nutné defragmentace úložiště, který bude zašifrováno. | ANO |
| Koncové zařízení je použitelné i v okamžiku kdy se úložiště zašifrovává. | ANO |
| Integrace s MS AD. | ANO |
| Zajištění úplného ověření před spuštěním systému včetně ověření pomocí služby Active Directory. | ANO |
| Centralizovaná správa všech zásad šifrování, včetně samošifrovacích disků a disků Microsoft BitLocker. | ANO |
| Přednastavené šablony zásad navržené pro snadné dodržování nařízení GDPR. | ANO |
| Možnost vynutit šifrovat na základě profilů koncových uživatelů, dat a skupin v rámci organizace. | ANO |
| Integrace řešení s ověřováním pomocí hesla systému Windows, otisků prstů a dalších. | ANO |
| GDPR – soulad s nařízením o ochraně osobních údajů. | ANO |
| Audit šifrování. | ANO |

## K14 – Zálohovací server s příslušenstvím

|  |  |
| --- | --- |
| **Parametr** | **Popis minimálního parametru** |
| **Základní a výkonová specifikace** | **Typ zařízení** |
| Server v provedení k instalaci do 19" racku, maximálně 2U |
| Zásuvné ližiny s managementem kabeláže |
| **Procesor** |
| 1ks CPU - architektura x86 v testu na cpubenchmark.net minimálně 40000 bodů. Max. počet CPU je omezen na 1 a max. počet jader je omezen na 16 jader z důvodu licencování OS a aplikací. |
| **Paměť** |
| 512GB, typu DDR5 s taktem 4800MT/s, Dual Rank |
| **Řadič disků** |
| Podpora SAS12, SATA6 disků  8GB NV Cache, se zálohováním při výpadku napájení  Podpora RAID 1,5,6,50,60  Sběrnici připojení k systému PCI-e Gen 4 |
| **Pevné disky** |
| Server musí být osaditelný min. 12x 3,5" disky, SAS, SATA a min. 2x 2,5" disky SAS, SATA. Dále min. 2x SSD na instalaci OS. Veškeré potřebné komponenty (řadič, diskové pozice, kabeláž, napájecí zdroje apod.) |
| Požadujeme dodat 8 ks min. 8TB SAS nebo SATA disků a 6 ks disků min. 3.84TB, SATA, Read Intensive, DWPD 1 |
| **OS Boot** |
| Musí být zajištěn dvojicí SSD v RAID1 a kapacitou min. 480GB |
| Disky musí být připojeny na jiný RAID řadič, než datové disky |
| **LAN konektivita** |
| Celkem 2x 2p 10/25GbE SFP28 portů včetně 2ks SFP+ MM modulů a 2ks SFP+ SM, včetně odpovídajících 2m kabelů LC/LC-LC/LC. Karty budou od stejného výrobce jako v HCI nodech. |
| Na kartě LOM (onboard) nezabírající PCI-e slot 1ks ethernet adapter 2x1GbE 1000BASE-T. |
| **Napájení a chlazení** |
| Server musí být vybaven redundantním napájením a chlazením, hot-plug vyměnitelné za provozu |
| 2ks hot-swap zdroje napájení dimenzované pro plné osazení serveru disky, CPU, RAM a PCIe zařízení, účinnost min. na úrovni Titanium dle certifikace 80 PLUS |
| **Funkční specifikace** | Server musí být osazen TPM 2.0 |
| Server musí disponovat kompletním out-of-band managementem s dedikovaným LAN portem 1GBase-T. Interní web-GUI managementu v HTML5, možnost ovládání pomocí CLI. |
| Management serveru nevyžaduje instalaci agenta, jak pro monitoring, tak pro update SW/FW/BIOS v jednotlivých HW komponentech serveru. Podpora HW profilů. Podpora IPv6. |
| Podpora hromadné konfigurace více serverů pomocí XML souborů (z USB, nebo síťovým PXE bootem), hesla v takovém souboru musí být hashovaná proti zneužití (zero touch deployment). |
| Základní deska či management serveru musí být vybaveny vlastním dedikovaným úložištěm pro umístění ovladačů potřebných pro instalaci OS, diagnostických nástrojů a také konfiguračních parametrů jednotlivých komponent pro případ výměny HW, aby nebylo nutné použití CD/DVD nebo jiných asistečních médií. |
| Firmware všech součástí serveru musí být kryptograficky podepsán tak, aby v rámci distribučního řetězce nemohlo dojít k jeho narušení nebo jeho alternaci. Autenticitu a integritu firmware nahraného v součástkách musí být možné ověřit nástrojem od výrobce nebo v managementu serveru. |
| Server musí umožňovat „lock-out“ BIOSu a firmware jednotlivých komponent tak, aby bylo zabráněno přepisu závadnou aktualizací. |
| Z důvodu bezpečnosti musí management serveru umožňovat zakázání (a opětovné povolení) nepoužívaných USB portů, změna stavu USB portu musí být možná bez nutnosti restartu serveru. |
| Je požadována funkcionalita secure-erase (zabezpečené smazání veškerých dat na serveru a jeho komponentách po jeho vyřazení). |
| Server vybavený alfanumerickým zobrazovačem stavu s možností nastavení management IP adresy. |
| Součástí managementu serveru musí být vestavěná funkcionalita call-home (server musí být schopen automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce). |
| Centrální management serverů musí disponovat analytickou komponentou, která musí umožnit kontrolu nastavení bezpečnostních pravidel serveru oproti šabloně bezpečnostních zásad (například kontrola sily administrátorských hesel, platnosti certifikátu, zapnutí TLS pro management konzoli serveru, vypnutí USB portů a další). Tyto šablony musí být nezávislé na modelu serveru výrobce. |
| Součástí nabízeného serveru musí být validovaná komponenta (extention) pro Microsoft Windows Admin Center (zjednodušená správa serverů jako samostatných hostitelů nebo je přímo spravovat jako clustery Microsoft Windows). Pokudkomponenta vyžaduje dodatečné náklady pro jeho funkčnost po dobu požadované záruky a technické podpory, musí být součástí nabídky. |
| **Záruka, záruční servis a technická podpora** | Je požadován záruční servis na dobu 5 let s reakční dobou na založený incident do konce následujícího pracovního dne (NBD). |
| Technickou podporu poskytuje výrobce serveru s přístupem k telefonické podpoře 24x7x365. |
| Servisní zásahy provádí technik s příslušnou znalostí, schválený výrobcem |
| Aktualizace systému dostupné min. po dobu záruky zdarma, nabízené přehledně v servisním portálu po zadání sériového čísla |
| Vadná datová média zůstávají ponechána po servisním zásahu zadavateli |

## K15 – Licence SW pro zálohování nově pořizovaných serverů

|  |  |
| --- | --- |
| **Parametr** | **Minimální parametry (v případě maximálního, nebo fixního parametru, je toto uvedeno)** |
| **Obecné požadavky** | Požadujeme licenčně pokrýt zálohování neomezeného množství VM pro 6 CPU, bez omezení zálohované kapacity |
| Software musí být licencován pomocí trvalé licence |
| Řešení musí podporovat hostitele spravované serverem VMware vCenter ve verzích 6.x, 7.x a 8.0 i samostatné ESXi hostitele. |
| Řešení musí podporovat zálohování všech operačních systémů, které jsou podporovány pro provoz na těchto hypervizorech |
| Řešení musí podporovat zálohování celých zařízení NAS, jednotlivých sdílených složek SMB a NFS a souborových serverů Windows a Linux |
| Řešení nesmí být závislé na jednom poskytovateli HW, virtualizační, nebo cloudové platformy, a to jak pro výpočetní část, tak pro část ukládání dat |
| Řešení musí podporovat hostitele spravované pomocí Microsoft System Center Virtual Machine Manager 2012 R2 až 2019, klastrové i samostatné hostitele Hyper-V |
| Řešení musí umožňovat ukládání záloh do různých diskových úložišť, souborových systémů, objektových úložišť, nebo deduplikačních diskových zařízení |
| Řešení musí umožňovat rozšíření logického úložiště o vrstvy pro automatické vytváření sekundární a archivní kopie záloh, zajišťující soulad s pravidlem 3-2-1 ukládání záloh |
| **Funkční požadavky** | Řešení musí umožňovat "single pass backup“ s možností vyloučit zpracování jednotlivých souborů a složek. „Jednoprůchodová záloha“ je vyžadována pro všechny druhy obnovení včetně granulárních obnov na úrovni aplikačních položek |
| Řešení musí mít mechanismy k úspoře objemu úložného prostoru pro ukládání záloh. Jejich využití musí být volitelné a nesmí omezit žádné funkcionality zálohování a obnovy dat |
| Řešení musí umožňovat kopírovat body obnovení a replikovat virtuální počítače do vzdáleného umístění pomocí technologie založené na vestavěné WAN akceleraci |
| Řešení musí umožňovat připojování a spouštění jakéhokoli skriptu pro zálohování před nebo po spuštěním zálohovací úlohy, nebo před a po snapshotu VM |
| Řešení musí podporovat technologie klonování datových bloků u souborových systémů pro Windows i Linux pro zajištění dalších úspor konzumované kapacity |
| Řešení musí nabízet samoobslužný portál, prostřednictvím kterého si uživatelé mohou obnovit soubory z GuestOS, nebo virtuální počítače, včetně jejich okamžitého spuštění ze souboru zálohy, či objekty MS Exchange a databází MS SQL, Oracle a PosgreSQL (včetně obnovení k zvolenému bodu v čase) |
| Řešení musí umožňovat samostatně škálovat výkonově i geograficky výpočetní, úložné i administrativní komponenty |
| Řešení musí využívat mechanismus sledování změn bloku. Pro všechny podporované hypervizory musí být implementace CBT certifikována výrobcem hypervizoru |
| Řešení musí umožňovat vytváření záloh integrací se snímky úložiště. Dále musí umožnit obnovu jednotlivých VM, souborů a položek aplikace z těchto snímků. Proces zálohy nemůže k připojení snímku použít dočasného hostitele. Popsaná funkce musí fungovat pro prostředí VMware vSphere s předpokládanou kompatibilitou pro následující pole: Dell, NetApp, HPE, HITACHI VANTARA, IBM, Lenovo, Fujitsu, Pure Storage, CISCO, DataCore |
| Řešení musí mít oficiální podporu pro VMware vSAN certifikovanou společností VMware |
| Řešení musí mít replikaci produkčních VM přímo z infrastruktury VMware vSphere, mezi hostiteli ESXi, včetně asynchronní nepřetržité replikace. Řešení musí navíc umožnit jako zdroj replikačních úloh využít soubory záloh |
| Řešení musí využívat všechny režimy přenosu zálohy podporované hypervizorem (network, hotadd, direct SAN a direct NFS) |
| Řešení musí být schopen vytvořit zálohu „ad-hoc“ pomocí nativní konzole nebo webového klienta vSphere |
| Řešení musí umožňovat paralelní zpracování virtuálních disků a jejich disků, včetně paralelní obnovy virtuálních disků v úplném režimu obnovy VM |
| Řešení musí umožňovat okamžitou obnovu více virtuálních strojů současně, přímo ze záložních souborů z libovolného bodu obnovení (vestavěný NFS server). Tato funkce musí být podporována pro prostředí VMware a Hyper-V a musí fungovat bez ohledu na hardware používaný k ukládání záložních souborů VM |
| Uvedená funkce musí umožňovat spuštění zálohy vytvořené z různých platforem (různých virtuálních, fyzických a veřejných cloudových virtuálních strojů) |
| Řešení musí umožňovat online migraci virtuálních počítačů, zpuštěných z úložiště záloh, do produkčního úložiště pomocí funkcí hypervizoru. Řešení musí také poskytovat svou vlastní funkci, která takové schopnosti poskytne |
| Řešení musí umožňovat prezentaci disků přímo ze záložního souboru do spuštěné VMware VM |
| Řešení musí umožňovat úplné obnovení VM, obnovu souborů VM nebo disků VM |
| Řešení musí umožňovat úplné obnovení VM přímo do Microsoft Azure, Azure Stack, Amazon EC2, Google Cloud Platform |
| Řešení musí umožňovat obnovu souborů na stroj operátora nebo přímo do produkční VM bez potřeby agenta nainstalovaného uvnitř VM. Během obnovy bez agentů nesmí existovat žádné omezení na velikost souboru ani omezení počtu souborů |
| Řešení musí podporovat granulární obnovení libovolného objektu a všech atributů tohoto objektu včetně hesla, GPO, AD configuration partition, AD integrovaných záznamů DNS, Microsoft System Objects, informací o certifikátu CA a AD Sites subnet |
| Řešení musí podporovat granulární obnovení Microsoft SQL 2008 a novějších, včetně databází s možností obnovení v čase (PiT), obnovy na úrovni tabulky, schéma |
| Řešení musí podporovat podrobné obnovení Microsoft Sharepoint Server 2013 a novějších. Možnost obnovit položky, weby, oprávnění |
| Řešení musí podporovat granulární obnovu databází Oracle s obnovou v čase (PiT) a podporou Oracle DataGuard. Toto musí být nabídnuto pro databáze spuštěné v operačních systémech Windows a Linux |
| Řešení musí umožňovat publikování MS SQL a Oracle DB přímo ze záložního souboru na spuštěný databázový server |
| Řešení musí umožňovat integraci nativního pluginu pro zálohování Oracle RMAN |
| **Požadavky v oblasti bezpečnosti** | Přístup do řídící konzole musí být chráněný vícefaktorovou autentizací bez nutnosti přístupu k internetu. |
| Řešení musí umožňovat vytváření záloh odolných vůči náhodnému, či úmyslnému smazání, nebo ransomware útokům na komoditním serverovém HW, nebo jakémkoliv S3-kompatibilním objektovém úložišti |
| Řešení nesmí použít centrální databázi pro ukládání jakýchkoli metadat deduplikace. Ztráta databáze nemůže způsobit, že záložní soubory budou nestabilní. Metadata deduplikace musí být uložena v záložních souborech |
| Řešení musí umožňovat pravidelné automatické testování obnovitelnosti záloh, včetně funkčnosti jednotlivých služeb a kontrolou obsahu na kybernetické hrozby pomocí řešení třetích stran |
| Řešení musí disponovat nástrojem pro analýzu konfigurace z pohledu bezpečnostních "Best Practices" doporučení |
| Řešení musí umožňovat vytvářet a spouštět izolované "Sandbox" prostředí pro provoz skupin VM ze záloh, replik i snímků diskových polí |
| Řešení musí nabízet šifrování celého síťového provozu mezi všemi komponentami a také šifrování souborů záloh "na cíli" na diskovém, cloudovém nebo páskovém úložišti |
| Součástí záloh musí být všechny informace, potřebné pro zajištění obnovy i v případě nedostupnosti původního zálohovacího serveru, nebo databáze s katalogem záloh |
| Řešení musí umožňovat automatizovanou dvoustupňovou obnovu virtuálních strojů, což umožňuje vložení vlastních skriptů za účelem změny dat před obnovením do produkčního prostředí |
| **Požadavky na monitoring a reporting** | Řešení musí poskytovat dohled nad chráněnou virtualizační platformou, poskytující včasná varování před výpadkem, nebo omezením dostupnosti produkčního prostředí |
| Řešení musí informovat, které VM nejsou chráněné dostatečně, nebo vůbec a zároveň kdy a jakým způsobem byl naposledy vytvořen bod obnovy |
| Řešení musí poskytovat možnost automatizovaných řešení chybových stavů |
| Řešení musí poskytovat funkce pro zasílání stavových hlášení do centrálního monitorovacího nástroje přes SNMP protokol |
| Řešení musí podporovat monitorování virtualizovaných prostředí VMware vSphere a Microsoft Hyper-V bez nástrojů třetích stran |
| Řešení musí podporovat dohled následujících systémů: VMware, ESXi 6.x, 7.x a 8.0 pro placené i bezplatné edice ESXi. Podporovaní hostitelé mohou být spravováni pomocí vCenter serveru nebo pracovat v samostatném režimu |
| Řešení musí podporovat dohled následujících systémů: Microsoft Server Hyper-V 2012, 2012R2, 2016, 2019 a 2022 pro placené i bezplatné edice. Podporovaní hostitelé mohou být spravováni SCVMM nebo pracovat v samostatném režimu |
| Řešení musí být certifikováno jako „VMware ready“ |
| Řešení musí poskytovat detailní výkonové a kapacitní charakteristiky komponent zálohovací infrastruktury, včetně zátěže procesorů, paměti, sítě a diskových úložišť |
| Řešení musí podporovat vytváření alarmů pro skupiny virtuálních počítačů i pro jednotlivé stroje |
| Řešení musí podporovat automatizované vytváření a zasílání reportů e-mailem |
| Řešení musí podporovat připojení více vSphere a Hyper-V serverů pro souběžné sledování různých virtualizovaných prostředí |
| Řešení musí obsahovat předdefinované alarmy a musí umožňovat vytváření nových alarmů a úpravu stávajících |
| Řešení musí mít centralizované řídicí panely (Dashboardy), které monitorují všechny objekty virtuální infrastruktury |
| Řešení musí podporovat monitorování HW komponent hostitelů virtualizace (ESXi, Hyper-V) |
| Řešení musí umožňovat monitorování zatížení zálohovacího serveru, množství chráněných dat, stav zálohovacích úloh, stav replikačních úloh a stav kontrolních úloh obnovitelnosti VM |
| Řešení musí poskytovat historická data a predikce z nich vyplývající, nezbytné pro plánování zdrojů pro provoz a ochranu virtualizovaného prostředí |
| Součástí řešení musí být i možnost vytvářet detailní auditové správy o změnách v konfiguraci zálohovacího řešení a o obnovách dat ze záloh |
| Řešení musí podporovat reporting virtualizovaných prostředí VMware vSphere a Microsoft Hyper-V bez nástrojů třetích stran |
| Řešení nesmí vyžadovat instalaci žádných agentů na monitorovaných hostitelích ESXi a Hyper-V a na virtuálních počítačích |
| Řešení musí umožňovat export sestav do formátů Microsoft Word, Microsoft Excel, Microsoft Visio a Adobe PDF |
| Řešení musí umožňovat plánování intervalů sběru dat a umožnit ad-hoc operaci sběru dat |
| Řešení musí mít reporty o plánování kapacity založené na scénářích „co-když“ |
| Řešení musí umožňovat vytváření personalizovaných sestav reportů v rámci jednoho dokumentu na základě podrobných údajů extrahovaných z předdefinovaných reportů |
| Řešení musí poskytovat možnost vytvářet náhledy v podobě webových dashboardů přizpůsobitelných zobrazovanými metrikami pro jednotlivé uživatele |
| **Podpora výrobce** | Bezplatný nárok na nejnovější firmware a aktualizace požadovaných funkcionalit, pokud jsou zpoplatněny, min. 60 měsíců |

## K16 – NAS s příslušenstvím

|  |  |
| --- | --- |
| **Parametr** | **Popis minimálního parametru** |
| **Základní a výkonová specifikace** | **Typ zařízení** |
| NAS server v provedení k instalaci do 19" racku, maximálně 2U |
| Zásuvné ližiny |
| **Procesor** |
| CPU - architektura x86, 64-bitová, s min. 4 plnohodnotnými jádry |
| **Paměť** |
| min. 8GB, typu DDR4 |
| min. 2 paměťové sloty, možnost rozšíření na 32GB |
| **Pevné disky** |
| Server musí být osaditelný min. 12 x 3,5" SATA HDD nebo 2,5" SATA SSD SATA disky |
| Požadujeme dodat 12 ks 8TB SATA disků, které jsou uvedeny na stránkách výrobce jako podporované |
| **LAN konektivita** |
| Min. 2x 10GbE SFP+ portů včetně 2ks 10G-BASE-SR modulů |
| Min. 1x 10GbE RJ-45 |
| Min. 2 x 1GbE RJ-45 |
| **Napájení a chlazení** |
| Zařízení musí být vybaveno redundantním napájením |
| 2ks hot-swap zdroje napájení vyměnitelné za provozu |
| **Funkční specifikace** | 2 x porty USB 3.2 Gen 1 |
| 1 x rozšiřovací port (Mini-SAS HD) |
| Systém je možné rozšířit na celkem 24x 3,5" SATA HDD |
| Podpora min. těchto síťových protokolů: SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI |
| **Záruka a technická podpora** | Je požadována záruka a záruční servis na dobu 5 let s výměnou HW následujícího pracovního dne (NBD). |
| Nárok na aktualizace systému dostupné min. po dobu záruky a záručního servisu. |

## K17 – licence SW serverového operačního systému

Zadavatel požaduje dodání následujících licencí:

|  |  |
| --- | --- |
| Microsoft Windows server Datacenter | 2x Microsoft Windows Server 2022 Datacenter pro HCI řešení – počet licencovaných jader musí pokrývat všechny jádra v nabízených HCI serverech |
| Microsoft Windows Server Standard | 1x Microsoft Windows Server 2022 počet licencovaných jader musí pokrývat všechny jádra v nabízeném zálohovacím serveru |

Je požadována dodávka licencí, jejichž pravost je garantovaná a ověřitelná u vlastníka autorských práv MICROSOFT.

Uchazeč zároveň poskytne dokumentaci, ze které bude jasný původ, resp. prodejní kanál licencí nebo zajistí zpracování smlouvy se společností Microsoft (Microsoft – SELECT Plus, Open, CSP, MPSA, EA) ve prospěch kupujícího.

Vyžaduje se dodání licencí formou licenčního portálu vázaného na koncového zákazníka (kupujícího), jehož součástí budou:

• Seznam nabízených licencí a jejich počet,

• Instalační médium,

• Instalační klíče,

• resp. další informace vztahujících se k licencím

Pro zdokumentování jasného původu požaduje zadavatel poskytnout dokumentaci obsahující označení prvního nabyvatele softwaru a také číslo smlouvy, pod kterou byl software pořízen, úplný řetězec vlastníků softwaru, potvrzení o odinstalaci od každého z předchozích vlastníků.

Jsou požadovány licence pro užití On-Premise.

**Zdůvodnění požadavku na kompatibilitu**

Zadavatel provozuje své technologické prostředí postavené na platformě OS Windows. Na této platformě je pak provozována majorita agendových informačních systémů zadavatele, které slouží k zajištění výkonu jeho činnosti a dále k zajištění interních činností a agend. Z těchto důvodů je požadována kompatibilita s tímto technologickým prostředím a jako definice požadavku je uveden konkrétní produktový název.

## K18 – server pro hyperkonvergovanou infrastruktur (HCI server) s příslušenstvím

|  |  |
| --- | --- |
| **Parametr** | **Popis minimálního parametru** |
| **Základní a výkonová specifikace** | **Typ zařízení** |
| Server v provedení k instalaci do 19" racku, maximálně 2U |
| Zásuvné ližiny s managementem kabeláže |
| **Procesor** |
| 1ks CPU - architektura x86 v testu na cpubenchmark.net minimálně 40000 bodů. Max. počet CPU je omezen na 1 a max. počet jader je omezen na 16 jader z důvodu licencování OS a aplikací. |
| **Paměť** |
| 512GB, typu DDR4 s taktem 4800MT/s, Dual Rank |
| **Pevné disky** |
| Server musí být osaditelný min. 24x 2,5" NVMe SSD a 2x SSD na instalaci OS. Veškeré potřebné komponenty (řadič, diskové pozice, kabeláž, napájecí zdroje apod.) musí být již nyní osazeny tak, aby server bylo možné funkčně osadit plným počtem SSD pouhým dodatečným vložením disků |
| Požadujeme dodat 8 ks disků min. 3,2TB, Enterprise, NVMe, Mix Used, DWPD 3, hot-swap |
| **OS Boot** |
| Musí být zajištěn dvojicí SSD v RAID1 a kapacitou min. 480GB |
| Disky musí být připojeny na jiný RAID řadič, než datové disky |
| **LAN konektivita** |
| Celkem 2x 2p 10/25GbE SFP28 portů včetně 2ks SFP+ MM modulů, 2ks SFP28 SM a odpovídajících 2m kabelů LC/LC-LC/LC. Síťové karty budou od stejného výrobce, plná kompatibilita s protokoly iWARP a RoCE v2 s pro technologii RDMA. |
| Na kartě LOM (onboard) nezabírající PCI-e slot 1ks ethernet adapter 2x1GbE 1000BASE-T. |
| **Napájení a chlazení** |
| Server musí být vybaven redundantním napájením a chlazením, hot-plug vyměnitelné za provozu |
| 2ks hot-swap zdroje napájení dimenzované pro plné osazení serveru disky, CPU, RAM a PCIe zařízení, účinnost min. na úrovni Titanium dle certifikace 80 PLUS |
| **Funkční specifikace** | Server musí být osazen TPM 2.0 |
| Server musí disponovat kompletním out-of-band managementem s dedikovaným LAN portem 1GBase-T. Interní web-GUI managementu v HTML5, možnost ovládání pomocí CLI. |
| Management serveru nevyžaduje instalaci agenta, jak pro monitoring, tak pro update SW/FW/BIOS v jednotlivých HW komponentech serveru. Podpora HW profilů. Podpora IPv6. |
| Podpora hromadné konfigurace více serverů pomocí XML souborů (z USB, nebo síťovým PXE bootem), hesla v takovém souboru musí být hashovaná proti zneužití (zero touch deployment). |
| Základní deska či management serveru musí být vybaveny vlastním dedikovaným úložištěm pro umístění ovladačů potřebných pro instalaci OS, diagnostických nástrojů a také konfiguračních parametrů jednotlivých komponent pro případ výměny HW, aby nebylo nutné použití CD/DVD nebo jiných asistečních médií. |
| Firmware všech součástí serveru musí být kryptograficky podepsán tak, aby v rámci distribučního řetězce nemohlo dojít k jeho narušení nebo jeho alternaci. Autenticitu a integritu firmware nahraného v součástkách musí být možné ověřit nástrojem od výrobce nebo v managementu serveru. |
| Server musí umožňovat „lock-out“ BIOSu a firmware jednotlivých komponent tak, aby bylo zabráněno přepisu závadnou aktualizací. |
| Z důvodu bezpečnosti musí management serveru umožňovat zakázání (a opětovné povolení) nepoužívaných USB portů, změna stavu USB portu musí být možná bez nutnosti restartu serveru. |
| Je požadována funkcionalita secure-erase (zabezpečené smazání veškerých dat na serveru a jeho komponentách po jeho vyřazení). |
| Server vybavený alfanumerickým zobrazovačem stavu s možností nastavení management IP adresy. |
| Součástí managementu serveru musí být vestavěná funkcionalita call-home (server musí být schopen automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce). |
| Centrální management serverů musí disponovat analytickou komponentou, která musí umožnit kontrolu nastavení bezpečnostních pravidel serveru oproti šabloně bezpečnostních zásad (například kontrola sily administrátorských hesel, platnosti certifikátu, zapnutí TLS pro management konzoli serveru, vypnutí USB portů a další). Tyto šablony musí být nezávislé na modelu serveru výrobce. |
| Součástí nabízeného serveru musí být validovaná komponenta (extention) pro Microsoft Windows Admin Center (zjednodušená správa serverů jako samostatných hostitelů nebo je přímo spravovat jako clustery Microsoft Windows). Pokud komponenta vyžaduje dodatečné náklady pro jeho funkčnost po dobu požadované záruky a technické podpory, musí být součástí nabídky. |
| **Záruka a technická podpora** | Je požadována záruka a záruční servis na dobu 5 let s reakční dobou na založený incident do konce následujícího pracovního dne (NBD). |
| Technickou podporu poskytuje výrobce serveru s přístupem k telefonické podpoře 24x7x365. |
| Servisní zásahy provádí technik s příslušnou znalostí, schválený výrobcem |
| Aktualizace systému dostupné min. po dobu záruky zdarma, nabízené přehledně v servisním portálu po zadání sériového čísla |
| Vadná datová média zůstávají ponechána po servisním zásahu zadavateli |

## K19 – Licence virtualizačního SW

Zadavatel požaduje dodání licencí, které zachovávají plnou kompatibilitu se stávajícím prostředím, když popis stávajícího prostředí je samostatnou přílohou zadávacích podmínek po podpisu NDA. Jde o dodání:

|  |  |
| --- | --- |
| VMware vCenter server¹ | 1× VMware vCenter Server 8 Foundation for vSphere up to 4 hosts (Per Instance) s Production podporou na 5 let |
| VMware vSphere ¹ | 3× VMware vSphere Standard 8 (1 CPU) s Production podporou na 5 let |

¹ Připouští se technicky a funkčně rovnocenné řešení. Řešení musí umožňovat migraci virtuálních serverů a jejich dat ze stávajícího virtualizačního prostředí postaveného na hypervizoru VMware ESXi do nově budované hyperkonvergované infrastruktury, a za chodu migrovaných virtuálních serverů bez výpadku dostupnosti jimi nabízených služeb. Dále musí být možné virtuální servery nejen migrovat z původní infrastruktury do nové (např. při hrozbě výpadku stávajícího virtualizačního řešení), ale také zpět do prostředí původního. Pokud se dodavatel rozhodne zahrnout do dodávky plnění na základě této technické specifikace jinou virtualizační platformu, než která je v prostředí zadavatel v současné době provozována (komponenty Vmware), je povinen provést migraci ze stávajícího virtualizačního prostředí (detail je uveden v samostatné příloze zadávací dokumentace „popis stávajícího technologického prostředí“), a to včetně všech v něm provozovaných virtuálních serverů a související infrastruktury. V případě takové migrace dodavatel negarantuje služby provozované v jednotlivých virtuálních serverech, u nichž si zadavatel zajistí úpravy sám mimo realizaci plnění dle této technické specifikace. V případě dodávky jiné virtualizační platformy není přípustné, aby dodané komponenty a technologie v rámci plnění této specifikace tvořili izolované virtualizační prostředí.

## K20 – UPS s příslušenstvím

|  |  |
| --- | --- |
| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění minimálně požadované funkcionality/vlastnosti** |
| Výkon [VA] | min. 5kVA |
| Výkon (kW) | Min.4,5kW |
| Výkonový záložní modul s podporou přídavných baterií | ANO |
| Provedení kombinované Rack/Tower | Rack max. 3U |
| Topologie | dvojitá konverze |
| Grafická indikace stavu | ANO |
| Elektricky oddělené skupiny zásuvek | ANO |
| Měření a ovládání jednotlivých skupin zásuvek | ANO |
| Hlučnost | Max. 45dB |
| Výstupní zásuvky | Svorkovnice + 2 skupiny 4 IEC C13 (10 A) + 2 IEC C19 (16 A) |
| Měření spotřeby elektrické energie v kWh | ANO |
| SMNP s Highest Cyber Security (UL 2900-2-2 compliant) | ANO |
| 1x slot pro rozšířenou komunikací osazený síťovou kartou (RJ45) s podporou protokolů: Fast ETHERNET, 10/100 Mbits, autonegotiation, HTTP 1.1, SNMP V1, SNMP V3, NTP, TFTP, SMTP, BOOTP/DHCP IPv6 Telnet, CLI,  SSH, ARP | ANO |
| Automatické rozpoznání přídavných baterií | ANO |
| 4 x reléový výstup - vzdálené odstavení a vzdálené zapnutí/vypnutí standardní součástí UPS | ANO |
| THDU | < 2% |
| Účinnost | min. 94% v režimu online (98% v režimu vysoké účinnosti) |
| Podpora správy přes webové prostředí | ANO |
| Možnost integrace managementu v rámci virtuálního prostředí | ANO |
| Instalace, připojení a oživení UPS, včetně úvodního nastavení síťové konfigurace | ANO |
| Bezpečnostní normy | IEC/EN 62040-1, UL 1778, CSA 22.2 |
| EMC parametry | IEC/EN 62040 -2, FCC Class A, IEC/EN 62040-3 |
| Homologace | CE, CB report (TUV), UL |
| Environmentální modul | ANO |
| Monitoring teploty | ANO |
| Monitoring vlhkosti | ANO |
| Monitoring sepnutých kontaktů | ANO |
| Možnost připojení dalších sond (primárně senzor zaplavení) | ANO |
| Slot pro síťovou komunikaci (RJ45) | ANO |
| Záruka | 3 roky |

## K21 – Rack s příslušenstvím

|  |  |
| --- | --- |
| **Položka** | **Popis minimálního parametru** |
| 3x rack 42U; demontáž staré kabeláže a montáž nových konektorů; přesun technologií. | **Rozvaděč serverovna - jídelna** |
| Demontáž kabelů a umístěných technologií ze starého racku. |
| Montáž a usazení 1x nového rozvaděče 42U, 800x800, uzamykatelný, odnímatelné bočnice, rackové PDU s 8 zásuvkami, skleněné dveře. |
| Nahradit starou optickou vanu s 24 optikami - osadit 1x novou optickou vanu 24p, při přesunu nutno zkrátit vyschlé optické kabely o cca 1,5m a znovu navařit optické konektory 24x. |
| Požadujeme konektory ST, broušení UPC, rozměr vlákna 62.5/125 µm, typ vlákna G.651.1, max. vložný útlum <0.3 dB. |
| 24x měření spoje OTDR včetně protokolu. |
| Nahradit starou optickou vanu s 12 optikami - osadit 1x novou optickou vanu 24p, při přesunu nutno zkrátit vyschlé optické kabely o cca 1,5m a znovu navařit optické konektory 12x. |
| 12x měření spoje OTDR včetně protokolu. |
| Přesunout 2x 24p RJ45 patch panel Panduit ze starého racku do nového. |
| Osadit 1x nový 24p patch panel RJ45 a do něj zakonektorovat kabely, které vedou do racku „napřímo“. |
| Požadujeme konektory RJ45, podporující protokoly 2.5G/5GBASE-T a nižší a splňující standardy ISO/IEC 11801 a ANSI/TIA 568.2-D. |
| Rozměry keystonu splňují požadavky z EN 60603-7 (je kompatibilní s modulárními zásuvkami různých výrobců). |
| Nepožadujeme certifikační protokoly na metalické spoje. Požadujeme funkčnost tras a zdokumentování technických parametrů metalických tras = celkem 48+24 = 72 portů RJ45. |
| Osadit 4x nový 1U vyvazovací panel plastový. |
| Osadit nový 1x kovový vertikální vyvazovací žlab 42U s krytem. |
| Požadujeme zajištění záložního připojení odpovídající úrovně po dobu realizace za provozu. |
| **Rozvaděč internát DM - A, místnost 03** |
| Demontáž kabelů a umístěných technologií ze starého racku. |
| Montáž a usazení 1x nového rozvaděče 42U, 800x800, uzamykatelný, odnímatelné bočnice, rackové PDU s 8 zásuvkami, skleněné dveře. |
| Nahradit starou optickou vanu s 24 portů - osadit 1x novou optickou vanu 24p, při přesunu nutno zkrátit vyschlé optické kabely o cca 1,5m a znovu navařit optické konektory 8x. |
| Požadujeme konektory ST, broušení UPC, rozměr vlákna 62.5/125 µm, typ vlákna G.651.1, max. vložný útlum <0.3 dB. |
| 8x měření spoje OTDR včetně protokolu. |
| Přesunout staré 3x 24p patch panely Cat5E do nového racku. Pokud staré patch panely nepůjde přesunout, tak kabelář v patch panelech odstříhat a osadit 3x nový RJ45 patch panel, znovu zaranžovat RJ45 porty s 4 kroucenými dvojlinkami – celkem 3x24 = 72 portů RJ45. |
| Osadit nový 1x 24p patch panel RJ45 a do něj zakonektorovat kabely, které vedou do racku „napřímo“. |
| Požadujeme konektory RJ45, podporující protokoly 2.5G/5GBASE-T a nižší a splňující standardy ISO/IEC 11801 a ANSI/TIA 568.2-D. |
| Rozměry keystonu splňují požadavky z EN 60603-7 (je kompatibilní s modulárními zásuvkami různých výrobců). |
| Nepožadujeme certifikační protokoly na metalické spoje. Požadujeme funkčnost tras a zdokumentování technických parametrů metalických tras = celkem 72+24 = 96 portů RJ45. |
| Osadit 4x nový 1U vyvazovací panel plastový. |
| Osadit nový 1x kovový vertikální vyvazovací žlab 42U s krytem. |
| **Rozvaděč internát DM - B, místnost 106** |
| Demontáž kabelů a umístěných technologií ze starého racku. |
| Montáž a usazení 1x nového rozvaděče 42U, 800x800, uzamykatelný, odnímatelné bočnice, rackové PDU s 8 zásuvkami, skleněné dveře. |
| Nahradit starou optickou vanu s 24 portů - osadit 1x novou optickou vanu 24p, při přesunu nutno zkrátit vyschlé optické kabely o cca 1,5m a znovu navařit optické konektory 12x. |
| Požadujeme konektory ST, broušení UPC, rozměr vlákna 62.5/125 µm, typ vlákna G.651.1, max. vložný útlum <0.3 dB. |
| 12x měření spoje OTDR včetně protokolu. |
| Nahradit staré 3x 24p patch panely Cat5E, které nepůjdou přesunout do nového racku. Kabelář v patch panelech odstříhat a osadit 2x nové 48portové RJ45 patch panely, znovu zaranžovat RJ45 porty s 4 kroucenými dvojlinkami – celkem 3x24 = 72 portů RJ45. Plus zaranžovat do patchpanelu 24 kabelů, které nyní vedou "napřímo". Celkem 72+24 = 96 x portů RJ45. |
| Požadujeme konektory RJ45, podporující protokoly 2.5G/5GBASE-T a nižší a splňující standardy ISO/IEC 11801 a ANSI/TIA 568.2-D. |
| Rozměry keystonu splňují požadavky z EN 60603-7 (je kompatibilní s modulárními zásuvkami různých výrobců). |
| Nepožadujeme certifikační protokoly na metalické spoje. Požadujeme funkčnost tras a zdokumentování technických parametrů metalických tras = celkem 72+24= 96 portů RJ45. |
| Osadit 4x nový 1U vyvazovací panel plastový. |
| Osadit nový 1x kovový vertikální vyvazovací žlab 42U s krytem. |
| Záruka | 2 roky |

V souvislosti s výše uvedenými požadavky na úpravu stávajícího rackového vybavení je ve lhůtě pro podání nabídek pořádána prohlídka místa plnění.

Žádáme dodavatele, pokud na základě prohlídky místa plnění navrhnou efektivnější formu realizace rackové připravenosti a jejich kapacity dle této kapitoly, aby případný návrh na úpravu parametrů na základě jejich odbornosti a realizované prohlídky místa plnění adresovali zadavateli jako žádost o dodatečné informace s návrhem úpravy této kapitoly, včetně zdůvodnění jimi navrhovaného efektivnějšího postupu a konkrétních parametrů jejich návrhu.

## K22 – Appliance pro analýzu bezpečnostní událostí

|  |  |
| --- | --- |
| **Parametr** | **Popis minimálního parametru** |
| **Základní specifikace** | VM appliance výrobce (HW appliance není akceptovatelná) |
| Virtuální appliance pro platformu VMware vSphere 8.0 a vyšší |
| **Výkonové požadavky** | Výkon logování min. 6GB za 1 den |
| **Funkční požadavky** | **Logovací funkce** |
| Musí se jednat o centrální logovací prvek pro dodávaná zařízení (FW) |
| Ukládání Syslog zpráv z jiných systémů |
| Vizualizace provozu |
| Možnost dostat se z vizuálního zobrazení proklikem na konkrétní logy |
| Realtime a historický náhled do logů |
| Korelace logů |
| Samostatná sekce týkající se hrozeb v síti |
| Podpora prohlížení statistických údajů nad logy |
| **Reporting** |
| Podpora reportů nad logy ve formátu HTML/CSV/XML/PDF |
| Generování reportů v pravidelných intervalech |
| Předefinované vzory pro reporty na nejčastější použití |
| Možnost vytváření vlastních reportů na základě konkrétních SELECT dotazů do databáze |
| Možnost úpravy reportů do vlastního designu – vlastní loga, texty, úprava hlavičky |
| **Další funkce** |
| Event Management - upozorňování na důležité informace z logů – emailem a snmp trapy, syslog zprávou |
| Předvytvořený dashboard pro využití dohledovým centrem |
| **Možnosti správy a komunikace** |
| Podpora SNMP v2, v3 |
| Podpora REST API |
| Správa přes webové rozhraní HTTPS |
| Administrátorské účty musí být možné konfigurovat lokálně nebo na vzdáleném serveru (LDAP, RADIUS, Tacacs+) |
| **Podpora výrobce** | Nárok na nejnovější firmware a aktualizace požadovaných funkcionalit, pokud jsou zpoplatněny, min. 60 měsíců |
| Technický support výrobce v režimu 24x7, min. 60 měsíců |

# Instalace a zprovoznění

V rámci předmětu plnění zadavatel požaduje provedení min. následujících služeb Součástí předmětu plnění jsou dále služby a práce prodávajícího se zařízeními a licencemi přímo související a nezbytné k řádnému uvedení předmětu plnění do provozu:

* dopravu jednotlivých komponent do místa plnění na adrese sídla zadavatele, když umístění jednotlivých technologií vyplývá z popisu stávajícího stavu a před realizací plnění bude kontaktní osoba kupujícího připravena na výzvu prodávajícího jednotlivé lokality na adrese sídla upřesnit
* zpracování prováděcí dokumentace před započetím instalace. Prováděcí dokumentace musí být schválena Zadavatelem a až následně může implementace pokračovat způsobem popsaným v dokumentu.
* zpracování a předání instalační dokumentace,
* zpracování a předání administrátorské dokumentace
* integrace nově dodávaných a dotčených stávajících zařízení,
* nasazení Microsoft Active directory
* migrace uživatelských identit ze stávajících systémů společnosti OpenText (dříve Microfocus, dříve Novell) do MS ActiveDirectory
* migrace zařízení školy do MS ActiveDirecory, zejména zapojení koncových stanic s OS Windows do nového doménového prostředí
* součinnost při migraci autentifikace aplikací do MS ActiveDirectory
* nasazení systému pro správu identit a řízení životního cyklu identit ve vazbě na personální systém a systém Bakaláři školy (součinnost stávajících dodavatelů zajišťuje kupující)
* nasazení systému ochrany koncových zařízení včetně systému centrální správy
* zpracování dokumentace stávajícího síťového prostředí, navržení a implementace segmentace vnitřní sítě a konfigurace NGFW včetně jeho části v podobě interního segmentačního firewallu, včetně případného prostředí školy – pro konfiguraci stávajících zařízení vyhotoví prodávající konfigurační parametry za předpokladu, že tyto prvky nebudou moci převzít konfiguraci automaticky z nově dodávaných technologií; konfigurace stávajících prvků není součástí tohoto plnění
* dodávka dokumentace konečného stavu
* integrace nových přepínačů do sítě školy
* nasazení 802.1x systému v dotčených částech infrastruktury školy
* nasazení bezdrátové sítě ve škole
* dodání nové serverové HCI infrastruktury
* dodání nové zálohovací infrastruktury a její nasazení pro ochranu datové základny školy
* Služby specifikované v dílčích oblastech níže

Požadujeme, aby práce mající dopad do fungování IT prostředí Zadavatele, byly prováděny výhradně mimo pracovní dobu (tedy byly prováděny v časech 17:00 – 6:00, případně mimo pracovní dny kdykoliv).

## Popis instalačních služeb

Zadavatel požaduje provést následující práce na dodaných technologiích a jejich příslušenství:

|  |
| --- |
| K1 - Firewall |
| Analýza současného stavu  Návrh úpravy segmentace vnitřní sítě školy  Realizace změn v segmentaci vnitřní sítě školy v případě nutnosti provedení readresace dodávaných zařízení a přípravy dokumentace pro další stávající zařízení jejichž konfiguraci provádí kupující  Návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií), a začlenění firewallu do LAN prostředí.  Provedení kompletního nasazení  Integrace s MS AD a systémem pro ověřování 802.1x |
| K2-K8 - Přepínače |
| Analýza současného stavu  Instalace a konfigurace dodaných zařízení  Přenesení konfigurace na nové zařízení  Konfigurace dle požadavků specifikovaných v cílovém konceptu  Otestování nakonfigurovaných vlastností (802.1x, vysoká dostupnost, logování)  Integrace se systémem pro řízení přístupu 802.1x |
| K9 – Licence SW pro řízení přístupu do sítě 802.1x |
| Analýza současného stavu  Vytvoření politik pro nově začleněné uživatele (domov mládeže)  Provedení kompletního nasazení na všech dotčených zařízeních drátové i bezdrátové sítě  Otestování politik a jejich případná úprava |
| K10 – WiFi přístupové body |
| Fyzická instalace bezdrátových bodů  Návrh rozdělení jednotlivých SSID  Vytvoření politik pro bezdrátovou část a také pro bezpečnostní mechanismy, včetně ověřování zařízení a uživatelů  Nastavení řízení přístupu a integrace se systémem 802.1x  Dokumentace |
| K11 – Licence SW nástroje pro řízení přístupových oprávnění – Identity management system |
| Napojení na zdrojové systémy  Provedení inicializačních přenosů  Kontrola struktury objektů a úprava přenosových politik  Napojení cílových systémů  Nastavení logování a auditu  Dokumentace |
| K12 – Licence SW ochrany koncových stanic a serverů (Anti-X) |
| Analýza současného stavu  Vytvoření politik pro dílčí typy koncových zařízení  Otestování politik  Vytvoření plánu nasazení na všech zařízeních školy  Provedení kompletního nasazení |
| K13 – Licence SW pro správu kryptografických prostředků |
| Analýza současného stavu  Vytvoření politik pro dílčí typy koncových zařízení (v MS AD)  Konfigurace systému MS Bitlocker  Vytvoření plánu nasazení na všech zařízeních školy  Provedení kompletního nasazení |
| K14+K15+K16 – HW a SW systém pro zálohování datové základny školy |
| Analýza současného stavu  Vytvoření politik pro zálohování, replikaci a retenci dat  Otestování politik  Vytvoření backup a restore plánu  Provedení kompletního nasazení |
| K17 – Licence SW serverového operačního systému |
| Instalace nového prostředí – migrace stávajících virtuálních serverů na nové verze provádí kupující nebo jeho dodavatelé informačních systémů užívající toto prostředí; součástí plnění proto není blíže neurčený rozsah migrovaných systémů s dopady do v nich provozovaných systémů a agend  Instalace MS ActiveDirectory v topologii doporučovanou výrobcem  Konfigurace MS ActiveDirectory ve vazbě na M365 a společné a synchronizované účty uživatelů v těchto platformách  Migrace poštovního serveru PostFix do poštovní služby M365 v rámci konfigurace nového prostředí (součástí bude spuštění oddělených mailových poddomén pro žáky, studenty a zaměstnance. Po spuštění nového prostředí bude zadavatel provozovat jediné mailové řešení a to M365. Je požadována migrace účtů i jejich obsahu, včetně pravidel a aktuálního obsahu schránek.  Instalace komponent potřebných pro provedení migrace ze systému Novell (viz níže)  Imagování OS pro učebny – Součástí dodávky a spuštění služeb doménového prostředí serverového operačního systému musí být i konfigurace nástroje, který umožní pro jednotlivé učebny vybavené několika počítači připravit image operačního systému včetně dalšího softwarového vybavení a tuto image automatizovaně rozdistribuovat na určené počítače učebny. Součástí dodávky pak bude dále i dokumentace umožňující přípravu a práci s takovými image a jejich distribuci a dále dokumentace popisující konfigurace nástroje pro tuto službu za účelem možnosti úpravy této služby do budoucna vlastními pracovníky zadavatele.  Provedení testů vysoké dostupnosti  Dokumentace |
| K18+K19 – Server HCI |
| Návrh a kompletní integrace serverové virtualizační platformy s nově dodaným serverem.  Implementace pořízených technologií.  Analýza možnosti přesunu dat a systémů (VM) ze stávajících serverů a sestavení doporučení pro zadavatele a jeho stávající dodavatele, jichž by se navrhovaná migrace týkala. Uvážení rozložení VM mezi stávající a nově dodané technologie a migrace určených částí na novou serverovou platformu a nové diskové úložiště.  Pokud se dodavatel rozhodne zahrnout do dodávky plnění na základě této technické specifikace jinou virtualizační platformu, než která je v prostředí zadavatel v současné době provozována (komponenty Vmware), je povinen provést migraci ze stávajícího virtualizačního prostředí (detail je uveden v samostatné příloze zadávací dokumentace „popis stávajícího technologického prostředí“), a to včetně všech v něm provozovaných virtuálních serverů a související infrastruktury. V případě takové migrace dodavatel negarantuje služby provozované v jednotlivých virtuálních serverech, u nichž si zadavatel zajistí úpravy sám mimo realizaci plnění dle této technické specifikace. V případě dodávky jiné virtualizační platformy není přípustné, aby dodané komponenty a technologie v rámci plnění této specifikace tvořili izolované virtualizační prostředí.  Začlenění nové serverové infrastruktury do stávajícího prostředí, konfigurace prvků vysoké dostupnosti.  Implementace automatické odstávky a najetí serveru v případě výpadku a obnovení dodávky elektrické energie.  Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy. |
| K20 – UPS |
| Fyzická instalace a zapojení obou UPS  Připojení do elektrické sítě  Konfigurace s virtualizačním systémem školy  Nastavení shut-down politik pro virtuální servery  Dokumentace  Elektrická revize (pokud je relevantní) |
| K21 – Rack s příslušenstvím |
| Provedení kompletní instalace racků a kabelových rozvodů včetně příslušenství  Začištění  Dokumentace |
| K22 – Appliance pro analýzu bezpečnostních událostí |
| Integrace s K1  Připojení dalších možných zdrojů dat ze stávajícího prostředí, dle analýzy a specifikace v rámci prováděcího projektu  Nastavení politik pro detekci anomálních stavů  Nastavení notifikací  Dokumentace |
| Migrace uživatelských identit ze systému Novell do MS ActiveDirectory (souvisí s K9, K11 a K17) |
| 1. Analýza a popis aktuálního stavu   * Zmapování současných adresářových a autentizačních služeb a jejich vazeb. * Analýza řízení uživatelských identit. * Analýza a popis základních síťových a souborových služeb a požadavků na jejich funkcionalitu. * Zmapování požadavků na správu AD prostředí. * Analýza poštovních/groupware služeb * Analýza koncových stanic a správy jejich životního cyklu * Analýza dalších provozovaných systémů a aplikací, a způsobu autentizace uživatelů   2. Návrh cílového stavu   * technická infrastruktura (doménové řadiče, sites, replikační topologie) * síťové služby (DNS, DHCP, NTP) * logická struktura AD * model řízení přístupu ke zdrojům * security model (password policy, audit policy, hardening, FGPP) * GPO model * harmonizace jmenných konvencí pro AD objekty * návrh řízení životního cyklu uživatelských identit   3. Realizace   * Implementace a konfigurace AD infrastruktury dle návrhu * Nasazení řešení pro správu identity (IdM systém)   + Napojení zdrojových systémů identit do IdM (IS Bakaláři, PERM)   + Napojení dalších požadovaných systémů do IdM dle této specifikace * Migrace objektů uživatelů z prostředí Novell do AD (cca 1500 uživatelů, z toho 230 zaměstnanců) * Napojení M365, synchronizace identit * Migrace objektů typu skupina do AD * Napojení systémů a ověření funkčnosti * Migrace koncových stanic do AD, včetně uživatelských nastavení (profilů) a dat (okolo 670 učitelských, resp. zaměstnaneckých stanic včetně počítačů na učebnách, mobilních učebnách; okolo 480 žákovských stanic, včetně mobilních učeben) * Začištění prostředí po migraci   4. Dokumentace, zaškolení, předání |

## Dokumentace

Zadavatel požaduje zpracování a předání níže uvedené dokumentace. Dokumentace musí být zhotovena v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. PDF, ODT atd.) na datovém nosiči a 1× v papírové formě.

### Prováděcí dokumentace

Prováděcí dokumentace bude sloužit jako podklad pro vlastní implementaci řešení do prostředí kupujícího, musí zahrnovat detailní popis cílového stavu a postupu implementace, včetně plánovaných změn v konfiguraci současné infrastruktury.

### Provozní dokumentace

Provozní dokumentace bude zpracována a předána v rozsahu detailního popisu skutečného provedení popisu činností běžné údržby a činností pro spolehlivé zajištění provozu.

## Zaškolení IT administrátorů

Prodávající zrealizuje v sídle kupujícího prezenční zaškolení pro IT administrátory kupujícího. Školení bude pokrývat všechny komponenty dodávané v rámci předmětu plnění, a to minimálně v rozsahu (1) běžných administrátorských činností pro implementované systémy, (2) standardní údržby systémů pro administrátory zadavatele a (3) základní identifikace nestandardních stavů systému a jejich příčin.

Minimální požadovaný rozsah zaškolení pro administrátory je 32 hodin. Součástí zaškolení je zpracování a předání školících materiálů ze strany prodávajícího.

Kupující pro účely zaškolení zajistí a zpřístupní učebnu vybavenou notebookem nebo PC, prezentační technikou (ve smyslu projektor, tabule pro psaní / kreslení) a dále zajistí konektivitu do vnitřní sítě kupujícího.

## Přílohy

Příloha č. 1 – Rozhraní informačního systému Bakaláři

Příloha č. 2 – Rozhraní informačního systému PERM3