3. Popis technických prostředků

oblast	Parametr	Popis povinného parametru	Popis způsobu naplnění povinného paramtru	odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru, nebo funkční, veřejně a bezplatně přístupný přímý odkaz na externí zdroj
2ks Firewall	Výrobce, model, označení	Uveďte	FortiGate FG-90G	fortigate-90g-series.pdf
	Provedení	Do racku 1U, včetně montážního kitu	FG-90G včetně Rack Mount Tray	fortigate-90g-series.pdf
	Porty	min. 8x GE RJ45 a zároveň min. 2ks 10 GE RJ45 nebo SFP+	Zařízení má 8 RJ45 1Gbe portů a dále 2x 10Gbe jak v provedení RJ45, tak SFP+	fortigate-90g-series.pdf
	NGFW	Min. základní funkce Next-generation firewall - viz https://en.wikipedia.org/wiki/Next-generation_firewall - firewall, aplikační firewall s DPI, IPS. Administrace na bázi "objektů" (aplikace, uživatelů, lokality apod.) namísto IP adres, portů apod.	zařízení plně odpovídá definici NGFW, jedná se o aplikační firewall s funkcemi IPS, IDS, umožnuje administraci na bázi objektů apod.	Converged Next-Generation Firewall (NGFW) and SD-WAN
	Počet současných spojení	min. 1,5 milionu	Zařízení umožnuje 3 milony současných připojení	fortigate-90g-series.pdf
	Propustnost SSL VPN	min. 1,4 Gbps, při licenčním nebo technickém omezení počtu klientů požadujeme min. 25 klientů	Propustnost SSL VPN je 1.4Gbps, počet VPN připojený není licenčně omezen	fortigate-90g-series.pdf

	Propustnost SSL inspekce	min. 2.6 Gbps	Prpustnost při zapnuté SSL inspekci je 2,6Gbps	fortigate-90g-series.pdf
	Propustnost firewallu	min. 27 Gbps pro pakety 512 bytů a větší	Propustnost firewallu pro pakety 512 byte a větší je 28Gbps	fortigate-90g-series.pdf
	Propustnost NGFW	min. 2,5 Gbps	Propustnost NGFW je 2,5 Gbps	fortigate-90g-series.pdf
	Propustnost IPS	min. 4.4 Gbps	Propustnost IPS je 4.5 Gbps	fortigate-90g-series.pdf
	Propustnost detekce škodlivého kódu	min. 2.1 Gbps	Propustnost detekce škodlivého kódu je 2,2 Gbps	fortigate-90g-series.pdf
	Logování	min. 7 dnů historie v zabezpečeném cloud prostředí	Firewall je možné připojit k FORTIANALYZERT M CLOUD, který umožnuje ukládání logů po dobu 7 dnů	SD-CloudServices-FortiAnalyzer.pdf
	Zabezpečení VPN	Umožňuje dvoufaktorové ověřování pomocí mobilní aplikace	Firewall umožňuje zabezpeční VPN dvoufaktorovým ověřováním s využití různých technologií MFA	fortigate-90g-series.pdf
	Virtualizace	min. 5 virtuálních kontextů	Firewall podporuje 10 virtuálních kontextů	fortigate-90g-series.pdf
	Vysoká dostupnost	Podporují režimy Active/Passive i Active/Active se společnou konfigurací v případě zapojení druhého firewallu	Zařízení disponuje funkcí High Availability Configurations Active-Active, Active-Passive, Clustering	fortigate-90g-series.pdf
	Dualstack	podpora současného běhu IPv4 a IPv6	Ano. Jedná se o základní vlastnost systému FortiOS	fortigate-90g-series.pdf

	Aplikační kontrola	detekce, monitoring, povolení či zakázání obvyklých síťových aplikací na základě signatury dané aplikace, nikoliv dle portu Kontrola komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S, …)	Ano. Jedná se o základní vlastnost systému FortiOS	fortigate-90g-series.pdf
	Antivir	Integrovaný antivirus, možnost volby různých databází signatur, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV detekce, možnost detekce tzv. Grayware (rootkit, malware, spywave, keylogger, atd)	Ano. Jedná se o základní vlastnost systému FortiOS	fortigate-90g-series.pdf
	Kategorizace a blokace provozu	založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorii na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne	Zařízení disponuje funkcí Web filter, která umožňuje kategorizaci webového obsahu dle zadání	fortigate-90g-series.pdf
	Antispam	antispamová a antivirová inspekce elektronické pošty	Ano. Jedná se o funkci FortiGuard Antispam Service popsanou na přiloženém odkazu v části FortiGuard AI-Powered Security Services. URL filtering s montorováním a kvótováním podle kategorií včetně časových intervalů. Automatická aktualizace kategorií.	fortigate-90g-series.pdf
	Sandbox	Možnost integrovaného sandbox (ověření škodlivosti kódu spuštěním v reálných operačních systémech) v zařízení nebo integrované rozhraní pro napojení na externí službu výrobce zařízení (služba není součástí dodávky)	Ano, jedná se o funkcionalitu FortiGuard Antivirus Security Service – FortiGuard Sandbox	fortigate-90g-series.pdf

	Aktualizace	automatická aktualizace bezpečnostních funkcí poskytovaná výrobcem zařízení	aktualizace firmware a bezpečnostních funkcí je zahrnuta v ceně dodaného řešení na dobu 60 měsíců a poskytována výrobcem zařízení	Součástí cenové nabídky
	Ověřování uživatelů	LDAP, Active Directory, Single Sign On vůči Active Directory, Radius, Ověřování na základě certifikátu	Autentizace vůči LDAP, AD včetně SSO, RADIUS i pomocí certifikátu. Jedná se o základní vlastnost systému FortiOS	fortigate-90g-series.pdf
	Management a monitoring	HTTP/S, SSH, SNMP, syslog	Správa a monitorování prostřednictvím http, https, ssh, SNMP i syslog. Jedná se o základní vlastnost systému FortiOS	fortigate-90g-series.pdf
	Záruka	min. 60 měsíců v režimu 24x7 poskytovaná výrobcem zařízení. Doručení náhradního zařízení max. následující den po nahlášení závady, včetně nároku na bezpečnostní aktualizace firmware a bezpečnostních funkcí - URL filtrace, IPS, antimalvare, antispam, aplikační kontrola)	60 měsíců Fortinet Unified Threat Protection (UTP) - IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and FortiCare Premium 24x7	Součástí cenové nabídky
Aktivní prvky - switche	Základní parametry	L2/L3 přepínač v rackovém provedení max. 1U, neblokovaná architektura	Společné parametry pro uvedené přepínače - jedná se vždy o L2/L3 přepínače v provedení do racku 1U využívající neblokovanou architekturu	FortiSwitch_Secure_Access_Series.pdf FortiSwitch_Data_Center_Series.pdf
	Agregace portů	podpora LACP	Switche podporují technologii LACP	FortiSwitch_Secure_Access_Series.pdf FortiSwitch_Data_Center_Series.pdf

	Směrování	hardwarové statické routování včetně VLAN, policy based routing	Směrování na bázi politk, hardwarové statické směrování včetně VLAN	FortiSwitch_Secure_Access_Series.pdf FortiSwitch_Data_Center_Series.pdf
	Řízení provozu	víceúrovňový QoS, podpora standardu 802.1p	IEEE 802.1p Based Priority Queuing, QoS ve více úrovních (fronty)	FortiSwitch_Secure_Access_Series.pdf FortiSwitch_Data_Center_Series.pdf
	VLAN	VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření	Podpora VLAN, 802.1Q, 802.1X Authentication (Port-based, MAC-based, MAB, Guest and Fallback VLAN, Dynamic VLAN Assignment) včetně aplikace QoS a ACL (access list - přístupové filtry)	FortiSwitch_Secure_Access_Series.pdf FortiSwitch_Data_Center_Series.pdf
	Ověřování uživatelů a zařízení	Podpora 802.1X	Zařízení podporují ověřování na základě 802.1x	FortiSwitch_Secure_Access_Series.pdf FortiSwitch_Data_Center_Series.pdf
	Základní parametry	L2/L3 přepínač v rackovém provedení max. 1U, neblokovaná architektura	Switch je L2/L3 v rackovém provedení 1U, nebloková architektura	FortiSwitch_Secure_Access_Series.pdf FortiSwitch_Data_Center_Series.pdf
	Dualstack	plný IPv4 a IPv6 dualstack včetně směrování a QoS	Plný dualstack IPv4 a IPv6 včetně směrování a QoS	FortiSwitch_Secure_Access_Series.pdf FortiSwitch_Data_Center_Series.pdf
	MAC	podpora min. 15 000 MAC adres	Zařízení podporují min 16.000 MAC adres	FortiSwitch_Secure_Access_Series.pdf FortiSwitch_Data_Center_Series.pdf
	Síťové toky	plný přímý export síťových toků - Netflow, IPFIX nebo ekvivalent (sFlow není ekvivalent)	Podporuje Flow Export (NetFlow i IPFIX)	FortiSwitch_Secure_Access_Series.pdf FortiSwitch_Data_Center_Series.pdf
	Monitoring a správa	plná podpora CLI, SSH, SNMP, syslog, sFlow, web rozhraní, REST nebo SOAP/WDSL API pro automatizaci (např. z IDM)	Plná podpora příkazové řádky CLI, ssh, SNMP, syslog, sFlow, http i https (web rozhraní), http REST API pro automatizaci a monitoring	FortiSwitch_Secure_Access_Series.pdf FortiSwitch_Data_Center_Series.pdf

	Nezávislý management	vyhrazený samostatný síťový port pro management (nezapočítává se do požadovaného počtu portů)	Vyhrazený port 1Gb FortiLink nad rámec stadndardních portů (out of band management), správa přes GUI, API nebo příkazový řádek	FortiSwitch_Secure_Access_Series.pdf FortiSwitch_Data_Center_Series.pdf
	Centrální správa	jednotná správa, monitorování a aktualizace firmware z centrální grafické konzole obsažené ve firmware nabízených síťových prvků.	Jednotná správa, monitorování a aktualizace z centrální grafické (webové) konzole obsažené ve firmware nabízených síťových prvků a firewallu (technologie FortiLink)	FortiSwitch_Secure_Access_Series.pdf FortiSwitch_Data_Center_Series.pdf
	Administrativní rozhraní	Centrální administrativní rozhraní je jednotné pro přepínače i nabízený firewall.	Centrální administrativní rozhraní je jednotné pro přepínače i nabízený firewall prostřednictvím technologie FortiLink.	FortiSwitch_Secure_Access_Series.pdf FortiSwitch_Data_Center_Series.pdf
	Stohování	pokročilé stohování s rozložením LAG (link aggregation group) mezi více přepínačů ve stohu - např. technologie MLAG (Multi-Chassis Link Aggregation nebo obdobná	Technologie MLAG (MCLAG) napříč přepínači, pokročilé stohování více přepínačů	FortiSwitch_Secure_Access_Series.pdf FortiSwitch_Data_Center_Series.pdf
	Záruka	Min. 60 měsíců poskytovaná výrobcem zařízením	Doživotní záruka (min. 60 měsíců) poskytovaná výrobcem zařízením	FortiSwitch_Secure_Access_Series.pdf FortiSwitch_Data_Center_Series.pdf
	Specifické parametry			
	Počty, porty a propustnost, napájení	2x centrální přepínač - 48x 1 Gb RJ-45 + 4x 10 Gb SFP+, 2x 40GE QSFP porty , propustnost min. 330 Gbps	FORTISWITCH 548D, 48x GE/RJ45 ports, 4x 10 GE SFP+ ports and 2x 40 GE QSFP+ propustnost 336 Gbps	fortiswitch-campus-series.pdf
		3 x přístupový přepínač - 48x 1 Gb RJ-45 + 4x 10 Gb SFP+, propustnost min. 175 Gbps	FORTISWITCH 148F, 48x GE RJ45 and 4x 10GE SFP+, propustnost 176Gbps	FortiSwitch_Secure_Access_Series.pdf

		3x přístupový přepínač - 48x 1 Gb RJ-45 + 4x 10 Gb SFP+, min 24x 1Gb porty PoE/PoE+ (802.3af/at), propustnost min. 175 Gbps, až 370W napájení portů, označenení výrobce a modelu	FORTISWITCH 148F-POE, 48x GE RJ45 and 4x 10GE SFP+, 24 portů s podporou PoE 802.3af/at, propustnost 176Gbps	FortiSwitch_Secure_Access_Series.pdf
32ks WiFi AP	Výrobce, model, označení	Uveďte	FortiAP 231G s podporou WiFi6. Součástí balení je držák	fortiap-series.pdf
	Základní funkce	Přístupový bod (AP) standardu Wi-Fi 6 včetně montážního materiálu na strop	FortiAP 231G s podporou WiFi6. Součástí balení je držák	fortiap-series.pdf
	Frekvence	min. 3 nezávislé radiové moduly činnost v radiovém pásmu 2,4 a 5 GHz současně, s podporou standardu OFDMA min. u 2 modulů	Tri-Radio 5 GHz + 2.4 GHz + scanning | 3 nezávislé antény	fortiap-series.pdf
	Architektura	Homogenní WiFi síť s rychlým a spolehlivým roamingem klientů, podpora Mesh (https://en.wikipedia.org/wiki/Wireless_mesh_network)	Podpora homogenní mesh architektury s rychlým a spolehlivým roamingem, řízení centrálním kontrolerem	fortiap-series.pdf
	Anténní systém	interní systém, optimalizovaný pro montáž na strop	Ano, má interní antény	fortiap-series.pdf
	Současná obsluha více klientů	Podpora MU-MIMO (Multi-User MIMO) - multi-user multiple input/multiple output	2x2 MU-MIMO | Up to 574 Mbps + 1201 Mbps + scanning, multi-user multiple input/multiple output	fortiap-series.pdf
	Přenosové rychlosti	5GHz min 1200Mbps, 2.4 GHz min. 550Mbps	Pro 5GHz 1201/ pro 2.4GHz 574 Mbps	fortiap-series.pdf

	Standardy	podpora standardů 802.3at, 802.11n, 802.11ax, 802.11k, 802.11n, 802.11r, 802.11v, Hotspot 2.0	802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11u, 802.11v, 802.11w, 802.11ac, 802.11ax, 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az	fortiap-series.pdf
	Multi SSID	podpora vysílání min. 8 SSID (WiFi sítí) na 2.4 i 5 GHz současně, podpora přiřazení každého SSID do samostatné VLAN	Podpora 16 SSID současně pro 5 i 2,4 GHz Přiřazení každého SSID do samostatné VLAN je součástí operačního systému	fortiap-series.pdf fortios-v7.4.4-release-notes.pdf
	Zatížení	min. 500 přiřazených (asociovaných) klientů na radiový modul	Až 512 klientů na rádio	fortiap-series.pdf
	Řízení zátěže	automatické rozkládání zátěže přístupových bodů předáváním klientů a automatickým směrováním klientů na 5 GHz (pokud klienti podporují)	AP podporují tzv loadbalancing se směrování do 5GHz sítě	fortiap-series.pdf
	Porty	min. 2x 1Gb, min 1x PoE s podporou standardů 802.3at a 802.3af, 1x USB 3	2x 1Gb z toho, min 1x PoE s podporou standardů 802.3at a 802.3af	fortiap-series.pdf
	Bezpečnost	trvalá detekce cizích přístupových bodů/klientů nezávislým radiem, spektrální analýza	Zařízení disponuje funkcí detekce cizích přístupových bodů/klientů nezávislým radiem, spektrální analýzou	fortiap-series.pdf fortios-v7.4.4-release-notes.pdf
	Kontroler	Centrální kontroler pro kompletní centrální správu WiFi infrastruktury a řízení jejího provozu včetně roamingu klientů součástí dodávky. Kontroler musí být provozován v interní síti zadavatele a být integrální součástí firmware nabízených síťových prvků. Grafické webové rozhraní pro správu.	AP spravovány centrálně pomocí integrované sítě WLAN nabízeného firewallu FortiGate a grafického webového rozhraní	fortiap-series.pdf

	Autentizace, autorizace	podpora standardu WPA3 (Wi-Fi Protected Access III), integrovaný portál pro autentizaci uživatelů (Captive portal), ověření klientů (min. hardware, uživatel, operační systém, certifikát) s využitím protokolu 802.1X	Podporuje standardy WPA™, WPA2™, and WPA3™ s 802.1x nebo Preshared key, WEP, Web Captive Portal, MAC blocklist & allowlist.	fortiap-series.pdf
	IoT a lokalizace	integrovaná hardwarová podpora standardu 802.15.4 (Zigbee) a BLE (Bluetooth Low Energy)	Podporuje ZigBee a BLE	fortiap-series.pdf
	Správa	plná podpora CLI, SSH, SNMP, syslog, web rozhraní, hromadná aktualizace firmware a konfigurace	Hromadná aktualizace fw a konfigurací prostřednictvím centrálního kontroleru ve firewallu, plná podpora příkazové řádky CLI, ssh, SNMP a syslog, grafické webové rozhraní (GUI)	fortiap-series.pdf
	Monitoring	detailní monitoring a diagnostika provozu v reálném čase - parametry připojení a komunikace klienta, stav přístupových bodů (počty klientů, vytížení kanálů, signál, cizí (rogue) přístupové body)	Podrobný monitoring a diagnostika provozu v reálném čase - parametry připojení a komunikace klienta, stav přístupových bodů (počty klientů, vytížení kanálů, signál, cizí (rogue) přístupové body) v konzoli firewallu	fortiap-series.pdf
	Úsporné napájení	podpora standardu 802.3az - Energy-Efficient Ethernet (EEE)	Podporovaný standard 802.3az	fortiap-series.pdf
	Záruka	záruka min. 60 měsíců poskytovaná výrobcem zařízením	Doživotní záruka, min 60 měsíců	fortiap-series.pdf
Nástroj pro ukládání	Výrobce, model, označení	Uveďte	Aricoma Logger (vlastní produkt)	Logger.pdf

auditních záznamů	Základní funkce	Sběr, ukládání a správu provozních a bezpečnostních informací a událostí ze sledovaných systémů	Integrovaný systém pro sběr, ukládání a správu provozních a bezpečnostních informací a událostí ze sledovaných systémů. Systém Loger je založený na open source bezpečnostní/SIEM platformě Wazuh s modifikacemi naší společnosti	Logger.pdf
	Protokoly sběru logů	syslog, TCP, UDP, HTTP, JSON	Systém podporuje sběr logů pomocí protokolů syslog, TCP/UDP, http, JSON a dalších, AMQP pomocí dodavatelem vytvořeného doplňku	Logger.pdf
	Sběr síťových toků	netflow kompatibilní dle nabízeného firewallu a centrálního přepínače	Systém podporuje sběr síťových toků nabízených přepínačů a stávajících firewallů prostřednictvím modulu doplněného naší společností (ElastiFlow)	Logger.pdf
	Zdroje logů	Min. REST API, textové soubory, Radius, Active Directory, MS SQL databáze, Windows Event Log - včetně rozšířených "Applications and Services Logs", síťové prvky - syslog a Netflow, ostatní aktivní prvky - syslog, SNMP trap, Office 365, Sysmon (windows)	Systém podporuje REST API, textové soubory, Radius, Active Directory, MS SQL databáze, Windows Event Log (včetně rozšířených "Applications and Services Logs"), syslog, netflow, SNMP trap, Office365, Windows Sysmon jako zdroje logů	Logger.pdf
	Parsování logů	I Integrovaný nástroj pro parsování logů. Možnost nahrání části logu, online vytváření parseru a snadné testování výsledku. Podpora vytváření opakovaně použitelných vzorků - např. definice IP adresy regulárním dotazem apod.	Systém obsahuje integrovaný nástroj pro parsování logů (Ruleset, Decoders) včetně podpory vytváření parserů a jejich testování. Možnost nahrání části logu, online	Logger.pdf

			vytváření parseru a snadné testování výsledku. Podpora vytváření opakovaně použitelných vzorků – např. definice IP adresy regulárním dotazem apod.	
	Retence	Uchovávání logů 6 měsíců, automatická retence logů a indexů	Systém umožňuje uchování logů minimálně pod dobu 6 měsíců, podporuje automatickou retenci logů a indexů.	Logger.pdf
	Geolokace	Podpora automatického doplňování logů o informaci o lokalitě podle IP adresy	Systém podporuje automatické doplňování logů o lokalitě/poloze podle IP adresy (geolokace, geoip)	Logger.pdf
	Normalizace logů	Sjednocení názvů shodných dat z různých zdrojů logů např. pro snadné vyhledávání napříč zdroji	Systém podporuje automatickou normalizaci logů – sjednocení názvů shodných dat/údajů z různých zdrojů – např. sourceip => ipsrc	Logger.pdf
	Rozšíření logů	Podpora rozšíření logů o vlastní statické a dynamické (kalkulované) položky integrovaným nástrojem.	Systém umožňuje rozšířit/doplnit logy o vlastní statické i dynamické (počítané) položky pomocí integrovaného nástroje.	Logger.pdf
	Bezpečnost	Podpora šifrované komunikace se zdroji (SSL apod.), ověřování zdrojů (TLS apod.)	Systém podporuje šifrovanou komunikaci se zdroji logů (např. SSL, https, ..) i ověřování zdrojů (např. TLS).	Logger.pdf
	Výkon	500 EPS (event per second), 5000 FPM (flows per minute)	Systém poskytuje na běžném hardware (serveru) výkon větší než 1000 EPS a 5000 FPM	Logger.pdf

	Dashboardy	Uživatelské vytváření dashboardů (pracovních desek) včetně možnosti využití grafických prvků (grafy, mapy, histogramy apod.) i strukturovaných dat (tabulek)	Systém umožňuje uživatelsky vytvářet dashboardy včetně možnosti využití grafických prvků (grafy, mapy, histogramy apod.) i strukturovaných dat (tabulek)	Logger.pdf
	Export dat	Export dat do csv - výsledky hledání	Systém podporuje export většiny zobrazených dat do csv, včetně výsledků hledání	Logger.pdf
	Kanály	Možnost vytváření kanálů - datových sad či toků - na základě pravidel (logických podmínek) a to i napříč různými zdroji. Podpora dalšího zpracování - tvorba alarmů, zobrazení na dashboardu, online odesílání do nadřazeného systému apod.	Systém podporuje vytváření kanálů/datových sad na základě pravidel (logických podmínek) a to i napříč různými zdroji logů. Podporuje další zpracování – tvorbu alarmů, zobrazení na dashboardu, online odesílání do nadřazeného systému apod.	Logger.pdf
	Alerty, notifikace	Podpora vytváření alertů - překročení okamžitých či kumulovaných hodnot, zasílaní upozornění	Systém umožňuje vytvářet alerty – upozornění na překročení okamžitých i kumulovaných hodnot	Logger.pdf
	Active Directory	integrace s Active Directory pro ověřování uživatelů, nastavení oprávnění administrator a operator	Systém podporuje integraci s Active Directrory / LDAP pro ověřování uživatelů. Podporuje nastavení uživatelských oprávnění, včetně úrovní administrátor (správce systému) a operátor (uživatel systému)	Logger.pdf
	Vyhledávání	Rychlé a intuitivní vyhledávání v záznamech napříč všemi zdroji i při velkých objemech dat (řády TB). Jednoduchý dotazovací jazyk. Rychlá vyhledávání či	Systém obsahuje výkonný vyhledávají nástroj, který umožňuje rychlé a intuitivní vyhledávání v záznamech	Logger.pdf

		filtrování bez tvorby dotazů - výběrem v kontextovém menu vybraného pole uloženého záznamu.	napříč všemi zdroji i při velkých objemech dat. Obsahuje jednoduchý dotazovací jazyk. Umožňuje rychlá vyhledávání či filtrování bez tvorby dotazů.	
	Ovládání	Intuitivní grafické rozhraní	Ovládání systému je prostřednictvím intuitivního grafického rozhraní dostupného prostřednictvím běžných prohlížečů – MS Edge, Chrome, Safari, Firefox apod.	Logger.pdf
	Kompatibilita	Podpora provozu v prostředí nabízené serverové virtualizace	Systém je podporován pro provoz v prostředí serverové virtualizace Hyper-V	Logger.pdf
	Ukládání dat	do databáze, případná databázová licence je součástí dodávky	Data jsou ukládána (a indexována) do databáze, která je součástí systému / dodávky.	Logger.pdf
	Výstupy	Možnost výstupů do nadřazeného systému pro účely vzdáleného expertního dohledu. Zabezpečený přenos vhodným protokolem	Sytém umožňuje přenášet vybraná data zabezpečeným/šifrovaným protokolem do nadřazeného systému pro účely vzdáleného expertního dohledu – např. SOC (Security Operations Center)	Logger.pdf
	Integrace	Nástroj musí mít podporu pro integraci se sysmon a zpracování jeho dat, systém tím pádem umí hlídat spuštěné příkazy přes powershell, procesy, CMD atd.	Nástroj má podporu pro integraci se sysmon a zpracování jeho dat, systém tím pádem umí hlídat spuštěné příkazy přes powershell, procesy, CMD atd.	Logger.pdf
	Detekce zranitelností	Řešení umí získávat informace o nainstalovaném software + o nasazených	Nástroj ukládá informace o obsahu monitorovaného systému a porovnává výsledky	Logger.pdf

		KB a díky tomu provádět kontrolu vůči seznamu vydaných zranitelností.	s databází známých zranitelnost (CVE)	
	Bezpečnostní funkce	Řešení skenuje monitorovaný systém a hledá malware, rootkity a neobvyklé chování	Řešené obsahuje intuitivní grafické rozhraní, databázi a bezpečnostní funkce jako je kontrola zranitelností a funkci skenování monitorovaných systémů, vyhledávání malware, rootkitů a neobvyklé chování.	Logger.pdf
	Záruka	Záruka na 60 měsíců včetně poskytnutí opravných verzí	Záruka 60 měsíců včetně poskytnutí opravných verzí.	Logger.pdf
Server pro hypervisor	Výrobce, model, označení	Uveďte	Server PowerEdge Dell R6615	PowerEdge_R6615_Specsheet.pdf
	Provedení	Provedení rack. Barevně označené hot-plug komponenty. Pro přístup ke všem komponentám není nutné nářadí. Uzamykatelný čelní panel.	Server optimalizovaný pro umístění do racku. Server má barevně označené hot-plug komponenty, zásuvné ližiny s managementem kabeláže a uzamykatelný čelní panel	PowerEdge-R6615-Technical-Guide.pdf PowerEdge_R6615_Specsheet.pdf
	CPU	Minimálně 1x procesor 16 jádrový. Výkon serveru dle http://www.spec.org: SPECrate®2017_int_base min. 177 bodů SPECrate®2017_fp_base min. 229 bodů	1x procesor, AMD AMD EPYC 9124 16-Core Processor. SPECrate®2017_int_base min. 177 bodů SPECrate®2017_fp_base min. 229 bodů	http://www.spec.org

	RAM	Min. 12 slotů pro DDR5 RDIMM Min. 128GB RAM ECC, min. 4800 MT/s Počet paměťových modulů a rozmístění musí být zvoleno pro optimální výkon s CPU.	Server obsahuje 12 slotů pro DDR5 v provedneí RDIMM a je osazen 4ks 32GB RDIMM, 4800MT/s Dual Rank. Počet RAM modulů a rozmístění je optimální pro výkon CPU	PowerEdge-R6615-Technical-Guide.pdf PowerEdge_R6615_Specsheet.pdf
	Boot Drive	Min. 2x SSD 960 GB, read intensive, samostatný HW řadič RAID1 Tyto disky nesmí zabírat pozice pro disky určené pro data Disky musí být typu hot-plug a přístupné z přední nebo zadní strany serveru.	Server je osazen BOSS-N1 controller card + with 2 M.2 960GB (RAID 1). Disky jsou hot-plug a přístupné ze zadní strany serveru. Disky nezabírají pozice určené pro data.	PowerEdge-R6615-Technical-Guide.pdf PowerEdge_R6615_Specsheet.pdf
	Diskový subsystém	Šasi serveru musí pojmout 10 HDD formátu 2.5", přístupných ve vyměnitelných hot-swap rámečcích z přední strany serveru Rozhraní disků SAS4, SATA, rotačních i SSD Osazení 8ks 2.4TB SAS 10K	Šasi serveru je 2.5" Chassis with up to 10 SAS4/SATA Drives including 4 Universal Slots, Front PERC 12. server je osazen 8x 2.4TB Hard Drive SAS ISE 12Gbps 10K 512e 2.5in Hot-Plug	PowerEdge-R6615-Technical-Guide.pdf PowerEdge_R6615_Specsheet.pdf
	RAID hardware	22.5 Gbps SAS, 12 Gbps SAS, and 6 Gbps SATA/SAS, RAID 0,1,5,6,50,60 zálohovaná zapisovací cache min. 8 GB	Server je osazen řadičem PERC H965i, zálohovaná zapisovací cache 8 GB DDR4 3200 MT/s cache, 8 GB DDR4 3200 MT/s cache, podporované typy disků jsou 22.5 Gbps SAS, 12 Gbps SAS, and 6 Gbps SATA/SAS. Gen3 (8 GT/s) and Gen4 (16 GT/s) NVMe. RAID levels 0, 1, 5, 6, 10, 50, 60	Perc12_Datasheet.pdf
	Interface	Min. 3x externí USB, z toho min. 1x USB 3.0 Dedikovaný USB management port	Server je osazen 3x USB konektory (2x USB 2.0 a 1x USB 3.0) z toho jeden je na čelním panelu s podporou bootování.	PowerEdge-R6615-Technical-Guide.pdf PowerEdge_R6615_Specsheet.pdf

		Min. 2x VGA port (jeden z každé strany serveru)	Server má VGA z přední a zadní strany serveru.	
	LAN	Min. 2x LAN 1Gbe nezabírající PCI-e slot Min. 2x LAN 10/25GbE SFP28	Server je osazen těmito NIC: Broadcom 5720 Dual Port 1GbE LOM, karta nezabírá PCI-e slot. Intel E810-XXV Dual Port 10/25GbE SFP28, OCP NIC 3.0, karta rovněž nezabírá PCI-e slot	PowerEdge-R6615-Technical-Guide.pdf PowerEdge_R6615_Specsheet.pdf
	Napájecí zdroje	2x napájecí zdroj max. 700 W, redundance, min. Platinum specifikace dle 80 PLUS https://cs.wikipedia.org/wiki/80_Plus	Server je osazen dvěma redundatními zdroji Dual, Hot-Plug, Power Supply Fully Redundant (1+1), 700W MM HLAC (ONLY FOR 200-240Vac) Titanium	PowerEdge-R6615-Technical-Guide.pdf PowerEdge_R6615_Specsheet.pdf
	Rozšiřující sloty	Min. 3ks PCI-e sloty - 2ks x16 Gen5 a 1ks x16 Gen4	Server je osazen riserem Riser Config 2, 3 x16 LP (2x Gen5)	PowerEdge-R6615-Technical-Guide.pdf PowerEdge_R6615_Specsheet.pdf
	Kompatibilita	Microsoft Windows Server® Red Hat® Enterprise Linux SUSE® Linux Enterprise Server VMware® ESXi	Microsoft Windows Server with Hyper-V Red Hat Enterprise Linux SUSE Linux Enterprise Server VMware ESXi Canonical Ubuntu Server LTS	PowerEdge_R6615_Specsheet.pdf

	Management a vzdálená správa	Stavové informace na čelním panelu s výraznou indikací nestandardních a chybových provozních stavů či parametrů (min. napájení, teplota, vada HDD). Aktivní indikace standardního provozního stavu. V případě závady zobrazuje její popis v textové formě. Vzdálená správa – dostupnost centrálního management prostředí serveru, nezávislého na spuštěné virtualizační platformě, či spuštěném operačním systému, vč. monitoringu, chybových hlášení emailem, vzdáleného a lokálního připojení (KVM) prostřednictvím dedikovaného LAN portu s podporou IPv4 a IPv6 Vzdálená správa musí disponovat vlastním management GUI, přístupným z běžných www prohlížečů. GUI musí být čistě v HTML5 a nesmí využívat dodatečných JAVA nebo ACTIVE-X komponent. Musí umožnit vzdálenou obrazovku s konzolí, možnost vzdáleného připojení ISO virtuální DVD a možnost vzdáleného připojení USB disku. Management serveru musí disponovat vlastním úložištěm pro firmware, ovladače a softwarové komponenty. Komponenty mohou být setříděny a organizovány do instalačních sad a mohou být použity pro	Na čelním panelu se nachází LCD panel zobrazující požadované informace. Server nabízí Integrovaný řadič Integrated Dell Remote Access Controller (iDrac) v edici Enterprise, který disponuje požadovanými funkcemi v kombinaci s centrálním managementem Dell OpenManage	PowerEdge-R6615-Technical-Guide.pdf iDrac9-User-Guide.pdf Dell-Openmanage.pdf

		obnovu či přeinstalaci vadného firmware. Centrální management serverů musí disponovat analytickou komponentou, která musí umožnit kontrolu nastavení bezpečnostních pravidel serveru oproti šabloně bezpečnostních zásad (například kontrola síly administrátorských hesel, platnosti certifikátu, zapnuti TLS pro management konzoli serveru, vypnutí USB portů a další). Tyto šablony musí být nezávislé na modelu serveru výrobce.		

	Bezpečnost	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. Server musí disponovat bezpečnostním systémem ověření komponent. Tento systém musí umožňovat ověřit, že mezi výrobou serveru a doručením k zákazníkovi nebyla konfigurace komponent serveru změněna ani upravena.	Server obsahuje iDrac v edici umožňující zakázání (a opětovné povolení) nepoužívaných USB portů, změna stavu USB portu musí být možná bez nutnosti restartu serveru. Server disponuje Server Secured Component Verification	iDrac9-security-configuration-guide.pdf Poweredge-Secured Component Verification.pdf
	Compliance	Centrální management serverů musí umožňovat „server bare metal“ deployment založený na šablonách (předdefinovaných konfiguracích pravidel, jejichž součástí je kromě samotného OS i konfigurace BIOS, RAID, LAN, MAC, WWN). Z bezpečnostních důvodů musí být možné naplánovat pravidelné provedení porovnání aktuálního stavu konfigurace serveru s aplikovanou šablonou automatizovaným způsobem, s automatickým zasláním reportu o výsledku porovnání emailem. je-li tato vlastnost licencována, požadujeme plnou licenci v ceně serveru.	Centrální management Dell OpenManage serverů Dell OpenManage umožňuje „server bare metal“ deployment založený na šablonách. Zároveň management umožnuje pravidelné provedení porovnání aktuálního stavu konfigurace serveru s aplikovanou šablonou automatizovaným způsobem, s automatickým zasláním reportu o výsledku porovnání emailem.	Dell-Openmanage.pdf

	Záruka a technická podpora výrobce	Záruka min. 60 měsíců Dostupnost podpory 24 hodin denně, 365 dní v roce Reakční doba do konce následujícího pracovního dne od nahlášení na linku podpory. Servis je poskytován přímo výrobcem hardware. Oprava v místě instalace hardware. Možnost automatického generování servisního incidentu přímo u výrobce hardware (server musí být schopen automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce). Podpora musí zahrnovat i nárok na aktualizace software a firmware pro komponenty serveru. Podpora prostřednictvím Internetu musí umožňovat ověření typu a délky záruky a stahování aktuálních ovladačů, firmware, software a manuálů z internetu adresně pro konkrétní zadané sériové číslo zařízení bez nutnosti vytvoření uživatelského účtu pro danou činnost.	Záruka 60 měsíců, oprava druhý pracovní den v místě instalace, nárok na podporu výrobce a nové verze software a firmware. Zařízení umožňuje automatického generování servisního incidentu přímo u výrobce hardware (zařízení je schopno automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce), díky záruce ProSupport, dostupnost podpory je 24 hodin denně, 365 dní v roce. Reakční doba do konce následujícího pracovního dne od nahlášení na linku podpory. Servis je poskytován přímo výrobcem hardware. Oprava v místě instalace hardware. Prostřednictvím Internetu je možné ověření typu a délky záruky a stahování aktuálních ovladačů, firmware, software a manuálů z internetu adresně pro konkrétní zadané sériové číslo zařízení bez nutnosti vytvoření uživatelského účtu pro danou činnost.	Součástí cenové nabídky https://www.dell.com/support/home/en-us PowerEdge-R6615-Technical-Guide.pdf PowerEdge_R6615_Specsheet.pdf Dell-SupportAssist.PDF Dell-prosupport-brochure.PDF
	Licence	Licence pro operační systém Microsoft Windows umožňující provoz neomezeného počtu virtuálních serverů stejné edice	CSP Windows Server 2025 Datacenter - 16 Core EDU	https://www.microsoft.com/en-us/windows-server/blog/2024/11/04/windows-server-2025-now-generally-available-with-advanced-security-improved-performance-and-cloud-agility/

Bezpečné úložiště	Výrobce, model, označení	Uveďte	Dell PowerEdge R360	
	Provedení	Provedení rack. Barevně označené hot-plug komponenty. Pro přístup ke všem komponentám není nutné nářadí. Uzamykatelný čelní panel.	Server optimalizovaný pro umístění do racku. Server má barevně označené hot-plug komponenty, zásuvné ližiny s managementem kabeláže a uzamykatelný čelní panel	PowerEdge-r360-specsheet.pdf PowerEdge-r360-technical-guide.pdf
	CPU	Minimálně 1x procesor 6 jádrový. Výkon serveru dle http://www.spec.org: SPECrate®2017_int_base min. 51 bodů SPECrate®2017_fp_base min. 48 bodů	1 procesor Intel® Xeon® E-2436 2.9G, 6C/12T, 18M Cache SPEcrate2017_int_base 68.3 SPECrate_fp_base 88.4	http://www.spec.org
	RAM	min. 16 GB, min. 3200 MT/s	Server je vybaven 16GB RAM 16GB UDIMM, 4800MT/s ECC	PowerEdge-r360-specsheet.pdf
	Úložiště firmware	Min. 2x SSD 480 GB, read intensive, samostatný HW řadič RAID1 Tyto disky nesmí zabírat pozice pro disky určené pro data Disky musí být typu hot-plug a přístupné z přední nebo zadní strany serveru.	Server je osazen BOSS-N1 controller card + with 2 M.2 480GB (RAID 1). Disky jsou hot-plug a přístupné ze zadní strany serveru. Disky nezabírají pozice určené pro data.	PowerEdge-r360-specsheet.pdf PowerEdge-r360-technical-guide.pdf
	Úložiště data	Min. 4x 8TB, 6Gbps, min. 7 200 ot/min	Server je osazen 4ks 8TB 7.2K RPM SATA 6Gbps 512e 3.5in Hot-plug Hard Drive	PowerEdge-r360-specsheet.pdf PowerEdge-r360-technical-guide.pdf
	RAID hardware	SAS 12Gb, RAID 1,5,6, zálohovaná zapisovací cache min. 8 GB	Server je osazen PERC H755 Adapter LP	Dell-perc11.pdf

	LAN	2x 1GbE RJ-45 + 2x 10 GbE SFP28 1x 1Gb RJ-45 - samostatný port pro vzdálený management	Server je osazen: 1x PowerEdge R360 Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM 1x Intel E810-XXV Dual Port 10/25GbE SFP28 Adapter, PCIe Low Profile Server disponuje jedním 1Gbe portem vhrazeným pro management serveru	PowerEdge-r360-specsheet.pdf PowerEdge-r360-technical-guide.pdf
	USB	min. 2 USB konektory - min. 1x verze 3.0, min. min 1x na čelním panelu s podporou bootování	Server je osazen 3x USB konektory (2x USB 2.0 a 1x USB 3.0) z toho jeden je na čelním panelu s podporou bootování. Server má VGA z přední a zadní strany serveru.	PowerEdge-r360-specsheet.pdf PowerEdge-r360-technical-guide.pdf
	Napájení	2x napájecí zdroj min. 600 W, redundance	Server je osazen redundatními zdroji - Dual, Hot-Plug, Power Supply Fully Redundant (1+1), 700W	PowerEdge-r360-specsheet.pdf PowerEdge-r360-technical-guide.pdf
	Souborový systém	XFS	Veeam Hardened Repository (VHR) bude instalováno se souborovým systémem XFS	Veeam_Hardened_repository.pdf
	Ochrana dat	min RAID5, automatická relokací vadných datových bloků	Ochrana dat je zajištěna hardwarovým RAID serveru, který podporuje automatickou relokaci vadných datových bloků disků	PowerEdge-r360-specsheet.pdf PowerEdge-r360-technical-guide.pdf Dell-perc11.pdf
	Management	Servisní modul s možnosti samostatného přístupu po management síti, možnost vzdálené klávesnice, myši a obrazovky bez nutnosti běhu OS, možnost zapínat a vypínat server, možnost bootování se	Server nabízí Integrovaný řadič Integrated Dell Remote Access Controller (iDrac) v edici Enterprise, který disponuje požadovanými funkcemi	iDrac9-security-configuration-guide.pdf

		vzdáleného média. Vyhrazený LAN port, podpora HTTP/S, SSH, SNMP, syslog. Okamžité a historické hodnoty teplot a napájení. Podpora vícefaktorového ověřování (autentizace)		
	Retence dat	programově nastavitelné retenční lhůty na uložený objekt (např. soubor), po dobu retence nelze objekt modifikovat	VHR umožňuje programově nastavit retenční lhůty na uložený objekt - typicky soubor zálohy, po dobu retence nelze objekt modifikovat	Veeam_Hardened_repository.pdf
	Redundance	redundantní rotační díly a napájecí zdroje	Server obsahuje redundantní rotační díly (disky) a napájecí zdroje	PowerEdge-r360-specsheet.pdf PowerEdge-r360-technical-guide.pdf
	Ochrana proti přepisu dat	režim WORM (Write Once - Read many times Memory)	VHR podporuje režim WORM	Veeam_Hardened_repository.pdf
	Kompatibilita	Kompatibilita se nabízeným zálohovacím systémem, podpora ukládání záloh, řízení jejich historie a řízení retenčních lhůt	VHR je přímo podporován stávajícím zálohovacím systéme Veeam Backup & Recovery včetně ukládání záloh, řízení jejich historie a řízení retenčních lhůt. VHR je nativní součástí „ekosystému“ Veeam Backup & Recovery	Veeam_Hardened_repository.pdf

	Management a vzdálená správa	Stavové informace na čelním panelu s výraznou indikací nestandardních a chybových provozních stavů či parametrů (min. napájení, teplota, vada HDD). Aktivní indikace standardního provozního stavu. V případě závady zobrazuje její popis v textové formě. Vzdálená správa – dostupnost centrálního management prostředí zařízení, nezávislého na spuštěné virtualizační platformě, či spuštěném operačním systému, vč. monitoringu, chybových hlášení emailem, vzdáleného a lokálního připojení (KVM) prostřednictvím dedikovaného LAN portu s podporou IPv4 a IPv6 Vzdálená správa musí disponovat vlastním management GUI, přístupným z běžných www prohlížečů. GUI musí být čistě v HTML5 a nesmí využívat dodatečných JAVA nebo ACTIVE-X komponent. Musí umožnit vzdálenou obrazovku s konzolí, možnost vzdáleného připojení ISO virtuální DVD a možnost vzdáleného připojení USB disku. Management zařízení musí disponovat vlastním úložištěm pro firmware, ovladače a softwarové komponenty. Komponenty mohou být setříděny a organizovány do instalačních sad a mohou být použity pro	Na čelním panelu se nachází LCD panel zobrazující požadované informace. Server nabízí Integrovaný řadič Integrated Dell Remote Access Controller (iDrac) v edici Enterprise, který disponuje požadovanými funkcemi v kombinaci s centrálním managementem Dell OpenManage	iDrac9-User-Guide.pdf Dell-Openmanage.pdf PowerEdge-r360-technical-guide.pdf

		obnovu či přeinstalaci vadného firmware. Centrální management zařízení musí disponovat analytickou komponentou, která musí umožnit kontrolu nastavení bezpečnostních pravidel serveru oproti šabloně bezpečnostních zásad (například kontrola síly administrátorských hesel, platnosti certifikátu, zapnuti TLS pro management konzoli serveru, vypnutí USB portů a další). Tyto šablony musí být nezávislé na modelu serveru výrobce.		

	Compliance	Centrální management zařízení musí umožňovat „server bare metal“ deployment založený na šablonách (předdefinovaných konfiguracích pravidel, jejichž součástí je kromě samotného OS i konfigurace BIOS, RAID, LAN, MAC, WWN). Z bezpečnostních důvodů musí být možné naplánovat pravidelné provedení porovnání aktuálního stavu konfigurace serveru s aplikovanou šablonou automatizovaným způsobem, s automatickým zasláním reportu o výsledku porovnání emailem. je-li tato vlastnost licencována, požadujeme plnou licenci v ceně serveru.	Centrální management Dell OpenManage serverů Dell OpenManage umožňuje „server bare metal“ deployment založený na šablonách. Zároveň management umožnuje pravidelné provedení porovnání aktuálního stavu konfigurace serveru s aplikovanou šablonou automatizovaným způsobem, s automatickým zasláním reportu o výsledku porovnání emailem.	Dell-Openmanage.pdf
	Záruka	Záruka min. 60 měsíců. Dostupnost podpory 24 hodin denně, 365 dní v roce. Reakční doba do konce následujícího pracovního dne od nahlášení na linku podpory. Servis je poskytován přímo výrobcem hardware. Oprava v místě instalace hardware. Možnost automatického generování servisního incidentu přímo u výrobce hardware (zařízení musí být schopno automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce). Podpora musí zahrnovat i nárok na aktualizace software a firmware pro komponenty serveru. Podpora prostřednictvím Internetu musí	Záruka 60 měsíců, oprava druhý pracovní den v místě instalace, nárok na podporu výrobce a nové verze software a firmware. Zařízení umožňuje automatického generování servisního incidentu přímo u výrobce hardware (zařízení je schopno automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce), díky záruce ProSupport, dostupnost podpory je 24 hodin denně, 365 dní v roce. Reakční doba do konce následujícího pracovního dne od nahlášení na linku podpory. Servis je poskytován přímo	Součástí cenové nabídky https://www.dell.com/support/home/en-us PowerEdge-r360-specsheet.pdf PowerEdge-r360-technical-guide.pdf Dell-prosupport-brochure.PDF

		umožňovat ověření typu a délky záruky a stahování aktuálních ovladačů, firmware, software a manuálů z internetu adresně pro konkrétní zadané sériové číslo zařízení bez nutnosti vytvoření uživatelského účtu pro danou činnost.	výrobcem hardware. Oprava v místě instalace hardware. Prostřednictvím Internetu je možné ověření typu a délky záruky a stahování aktuálních ovladačů, firmware, software a manuálů z internetu adresně pro konkrétní zadané sériové číslo zařízení bez nutnosti vytvoření uživatelského účtu pro danou činnost.	
Záložní napájecí zdroj pro serverovnu	Provedení	do racku, včetně montážních ližin	Eaton 9SX 3000i Rack2U	Eaton-9px-3000.pdf
	Kapacita výstupního výkonu	Min. 2700 W / 3000 VA	Kapacita výstupního výkonu [W]: 2700, Kapacita výstupního výkonu [VA]: 3000	Eaton-9px-3000.pdf
	Výstupní napětí	230V	Vstupní napětí [V]: 200-276	Eaton-9px-3000.pdf
	Výstupní zásuvky	Min 8x IEC 320 C13	Výstupní přípojky: (8) IEC-320-C13, (1) IEC-320-C19	Eaton-9px-3000.pdf
	Síťová karta	min. 1x LAN base-T pro komunikaci se zařízeními	síťový management na samostatné kartě 1x Base-T - Eaton Komunikační karta M3 - Gigabit Network Card s podporou protokolů HTTPS1.1, MQTTS, TLS1.2, SNMPv1, SNMP v3, NTP, SMTPS, BOOTP/DHCP, CLI, SSH, ARP and Syslog a	Eaton-9px-3000.pdf

			IPv4/v6, TLSv1.2, HTTP(S)v1.1, NTP, SMTP(S), BOOTP/DHCP, SSH, SysLog(S), LDAP, AD, RADIUS	
	Stavové diody	pro vzdálené monitorování a řízení UPS. Podpora SNMP v3, HTTPS, IPv6	Na předním panelu jsou stavové diody indikující stavy: Napájen ze sítě, napájen z baterie, nutno vyměnit baterie, přetížení UPS atd.	Eaton-9px-3000.pdf
	LCD display	min. indikující stavy: Napájen ze sítě, napájen z baterie, nutno vyměnit baterie, přetížení UPS	Na předním panelu jsou stavové diody indikující stavy: Napájen ze sítě, napájen z baterie, nutno vyměnit baterie, přetížení UPS atd.	Eaton-9px-3000.pdf
	Battery Pack	zobrazující min. kapacitu baterie, účinnost, zatížení UPS, spotřebu energie. Možnost nastavení základních parametrů UPS včetně konfigurace výstupních zásuvek a nastavení zvukových upozornění	Na předním panelu je grafický LCD zobrazující min. kapacitu baterie, účinnost, zatížení UPS, spotřebu energie. Možnost nastavení základních parametrů UPS včetně konfigurace výstupních zásuvek a nastavení zvukových upozornění	Eaton-9px-3000.pdf
	Rozšiřitelnost	Včetně jednoho battery packu, který při 100% zátěži prodlouží provoz o min. 35 minut	Konfigurace je včetně Eaton Externí baterie pro 9PX 72V RT3U	
	Účinnost	Možnost připojení dalšího externího battery packu (není součástí dodávky)	Možnost připojení dalších až 4 EBM . Účinnost 98%	Eaton-9px-3000.pdf

	Záruka UPS	Min 5 let na zařízení i na baterie. U baterií akceptujeme záruku vztahující se pouze na závady, nikoliv na sníženou dobu zálohy.	Záruka na 5 let na zařízení i na baterie.	Součástí nabídkové ceny
1ks Záložní napájecí zdroje pro ostatní rozvaděče	Provedení	do racku, včetně montážních ližin	do racku 1U, včetně montážních ližin	https://www.eaton.com/cz/cs-cz/skuPage.5P1550IR.html
	Kapacita výstupního výkonu	Min. 1100 W / 1550 VA	Kapacita výstupního výkonu [W]: 1100, Kapacita výstupního výkonu [VA]: 1550	https://www.eaton.com/cz/cs-cz/skuPage.5P1550IR.html
	Výstupní napětí	230V	230 V (+6/-10 %) nastavitelné 200 V / 208 V / 220 V / 230 V / 240 V), 50/60 Hz +/- 0,1 % (automatická detekce)	https://www.eaton.com/cz/cs-cz/skuPage.5P1550IR.html
	Výstupní zásuvky	Min 6x IEC 320 C13	Výstupy Rack 1U model 6 IEC C13 (10A)	https://www.eaton.com/cz/cs-cz/skuPage.5P1550IR.html
	Síťová karta	slot pro volitelnou komunikační kartu	Model obsahuje 1 slot pro Network-MS, ModBus-MS nebo Relay-MS	https://www.eaton.com/cz/cs-cz/skuPage.5P1550IR.html
	Výstupní účiník	alespoň 0,7	Výstupní účiník 0,7	https://www.eaton.com/cz/cs-cz/skuPage.5P1550IR.html
	LCD display	Vícejazyčný grafický LCD displej	Vícejazyčný grafický LCD displej	https://www.eaton.com/cz/cs-cz/skuPage.5P1550IR.html
	Další porty	USB, RS232, mini svorkovnice	1 USB port + 1 RS232 sériový port a reléové kontakty (1 mini svorkovnice pro dálkové zapnutí a vypnutí a pro dálkové odstavení (RPO)	https://www.eaton.com/cz/cs-cz/skuPage.5P1550IR.html
	Účinnost	97	UPS 5P má energetickou účinnost až 98%	https://www.eaton.com/cz/cs-cz/skuPage.5P1550IR.html

	Záruka UPS	Min 5 let na zařízení i na baterie. U baterií akceptujeme záruku vztahující se pouze na závady, nikoliv na sníženou dobu zálohy.	5 let	https://www.eaton.com/cz/cs-cz/skuPage.5P1550IR.html
NAS pro zálohování a logy	Provedení	Volně stojící	Synology DS1621+	Synology_DS1621_Plus_DataSheet_enu.pdf
	Počet pozic na disky	Min. 6 x 3,5" nebo 2,5" SATA HDD/SSD	Zařízení je v provedení, které umožňuje osadit až 6 3,5HDD v provedení SATA HDD/SSD	Synology_DS1621_Plus_DataSheet_enu.pdf
	Procesor	Min. 4 jádrový s frekvencí min. 2,2 GHz	AMD RyzenTM V1500B quad-core 2.2 GHz	Synology_DS1621_Plus_DataSheet_enu.pdf
	Operační paměť	Min 4 GB DDR4, 1 volný slot pro další rozšíření	4 GB DDR4 ECC SODIMM (expandable up to 32 GB)	Synology_DS1621_Plus_DataSheet_enu.pdf
	Rozšiřující jednotky	Možno připojit expanzní polici pro min. 5ks HDD	DS1621+ podporuje až dvě expanzní jednotky Synology DX517 (5x 3,5" SATA HDD/SSD)	Synology_DS1621_Plus_DataSheet_enu.pdf
	Porty	Min 4x 1GbE LAN RJ-45 s podporou Link Aggregation Min 2x 10GbE LAN SFP+ min. 3x USB 3.0 nebo novější	Zařízení obsahuje v základu 4 x 1GbE RJ-45 a je dále doplněno o 2x 10Gbe LAN SFP+	Synology_DS1621_Plus_DataSheet_enu.pdf
	Rozšiřující porty	Min. 1x PCIe Gen3	Zařízení obsahuje 1x x 4-lane x8 slot PCIe 3.0 slots	Synology_DS1621_Plus_DataSheet_enu.pdf
	Podpora RAID	Min. RAID 0,1,5,6,10, podpora Global HotSpare	Synology Hybrid RAID (SHR), Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10	Synology_DS1621_Plus_DataSheet_enu.pdf
	Podpora změny RAID	Min. z RAID 5 na RAID 6	Zařízení podporuje nejen změnu z RAID5 na RAID6, ale i další varianty	Change the RAID Type of a Storage Pool | DSM - Synology Knowledge Center
	iSCSI	Počet cílů iSCSI target min. 120, počet jednotek iSCSI LUN min. 250	Maximální počet iSCSI target je 128, iSCSI LUN je maximum 256	Synology_DS1621_Plus_DataSheet_enu.pdf

	Podpora mezipamětí SSD	Ano po přidání M.2 SSD (není součástí dodávky)	Zařízení je možné osadit M.2 SSD disky	Synology_DS1621_Plus_DataSheet_enu.pdf
	Síťové protokoly	Min. SMB, NFS, FTP, iSCSI, SNMP	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP)	Synology_DS1621_Plus_DataSheet_enu.pdf
	Disky	Min. 4 disků uvedených v compatibility listu nabízeného NAS zařízení, každý o hrubé kapacitě min. 12TB, počet otáček min. 7200 rpm, rozhraní SATA 6Gb/s	Zařzení je osazeno 4x Synology HAT5300/ 12TB/ HDD/ 3.5"/ SATA/ 7200 RPM/ 5R	Synology_DS1621_Plus_DataSheet_enu.pdf
	Podpora zálohování O365	Ano - programové vybavení pro zálohování prostředí O365 je součástí zařízení	Zařízení obsahuje SW výbavu v podobě	SynologyABM365_Deployment_Recommendations_enu.pdf
	Záruka na NAS i disky	5 let	Zařízení je pokryté 5 letou zárukou, včetně disků	Součástí nabídkové ceny
Systém pro správu identit (Identity management - IDM)	Základní funkce	IDM (dále IDM nebo Systém) bude udržovat a spravovat identity a organizační strukturu organizace - třídy, učitelský sbor, administrativa atd. Spravované identity budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy. Identity budou ukládány v databázi. Systém bude spravovat i identity externích uživatelů (spolupracovníků a partnerů) využívajících ICT systémů zadavatele.	Vlastní produkt AC Identita – IDM (dále IDM nebo Systém) bude udržovat a spravovat identity a organizační strukturu organizace - třídy, učitelský sbor, administrativa atd. Spravované identity budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy. Identity budou ukládány v databázi.	ACIdentita.pdf

	Licence	Trvalá licence, která umožní nasazení a provoz IDM bez omezení na počet uživatelů, spravovaných identit a napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Zadavatele (počet záznamů, velikost databází atd.). Předpokládaný počet spravovaných identit je min 1000.	Dodaná trvalá licence umožní nasazení a provoz IDM bez omezení na počet uživatelů, spravovaných identit a napojených systémů a nijak neomezuje obvyklé nasazení a provoz s ohledem na charakter organizace objednatele. Počet spravovaných uživatelů není omezen.	ACIdentita.pdf
	Uživatelské rozhraní	Uživatelské rozhraní bude realizováno jako webový portál (dále jen Portál) dostupný z běžných prohlížečů (Edge, Chrome) a umožní přístup k datům a funkcím Systému i jeho správu a konfiguraci.	Řešení má kompletní uživatelské rozhraní jako webový portál ze kterého lze provádět konfigurační změny, přistupovat k datům, funkcím systému apod.	ACIdentita.pdf
	Evidence aplikací a rolí	Integrovaný registr aplikací a informačních systémů (souhrnně IS) a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby a zařazování uživatelů do rolí v příslušných IS	Systém obsahuje registr aplikací a informačních systémů a jejich uživatelských rolí. Role je možné importovat přes webové služby.	ACIdentita.pdf
	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.	Systém obsahuje podrobnou databázovou historizaci – evidenci všech změn identit identit včetně referenčních objektů a vazeb mezi nimi. Umožňuje poskytování dat v libovolném časovém okamžiku v minulosti i aktuálním.	ACIdentita.pdf
	Automatizace	Podpora tvorby pravidel v grafickém prostředí pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě libovolných atributů	Systém obsahuje grafické prostředí pro intuitivní tvorbu pravidel pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování	ACIdentita.pdf

		identity a přidružených referenčních objektů (třída, organizační jednotka, aplikační role, pracovní pozice atd.).	aplikačních rolí uživatelům na základě libovolných atributů identity a přidružených referenčních objektů (třída, organizační jednotka, aplikační role, pracovní pozice atd.).	
	Logování	Integrování logování min. následujících typů událostí: - události systému včetně webových služeb (aplikační log) - změny entit evidovaných systémem a změny konfigurace systému (auditní log) - synchronizace s napojenými systémy (synchronizační log) - odeslané notifikace a upozornění (notifikační log) Logy musí být dostupné nabízenému logovacímu systému nebo do něj exportovány	Systém umožňuje podrobné logování událostí, včetně: - 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) Systém poskytuje logy ve formátu vhodném pro nabízený systém pro sběr a správu logů.	ACIdentita.pdf
	Referenční objekty	Systém umožní přidávání a správu libovolných typů referenčních objektů a to i v průběhu správy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity. Základní (předpřipravené) referenční typy objekty budou min. pracovní pozice, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role.	Systém umožňuje přidávání a správu dalších typů referenčních objektů i v průběhu správy konkrétní identity s možností okamžitého použití referenčního objektu u právě spravované identity. Systém obsahuje připravené referenční objekty typu pracovní pozice, organizační jednotka, skupina, funkce, aplikace, skupina aplikací, aplikační role, certifikát a další.	ACIdentita.pdf

	Popisné atributy	Systém umožní dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IDM.	Systém umožňuje rozšiřování identit a referenčních objektů o další atributy a publikuje nové atributy externím aplikacím prostřednictvím rozhraní webových služeb	ACIdentita.pdf
	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).	Portál umožňuje 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).	ACIdentita.pdf
	Aktivní uživatelé	Systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem	Systém obsahuje přehled uživatelů aktuálně pracujících s Portálem	ACIdentita.pdf
	Slučování identit	Systém umožní sjednocení více uživatelů (identit) do jedné a odpovídající sjednocení spravovaných účtů.	Systém plně podporuje slučování uživatelů/identit včetně sjednocení navázaných spravovaných účtů.	ACIdentita.pdf
	Oprávnění	Víceúrovňová správa administrátorských oprávnění s možností nastavení oprávnění min. na úrovni organizační jednotky (nebo hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení pracovní pozice, přiřazení aplikační role, editace identity apod.)	Systém má integrovánu víceúrovňovou správu administrátorských oprávnění s možností nastavení oprávnění na úrovni organizační jednotky včetně podřízených struktur a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, přiřazení aplikační role, editace identity apod.)	ACIdentita.pdf

	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.	IDM umožňuje přiřazení rolí konkrétní identitě, pracovní pozici, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení platnosti přiřazení. Po vypršení platnosti přiřazení IDM rolí přiřazenému objektu automaticky odebere.	ACIdentita.pdf
	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.	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.	ACIdentita.pdf
	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.	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.	ACIdentita.pdf
	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.	IDM má 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.	ACIdentita.pdf

	Obnovení hesla	IDM bude obsahovat samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživatele musí být možno provádět min. pomocí SMS (tj. IDM musí být možné na SMS bránu či službu napojit). Rozhraní musí umožnit i běžnou změnu hesla (bez resetu).	IDM obsahuje samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživateli je možné provádět pomocí SMS (tj. IDM je možné na SMS bránu či službu napojit). Rozhraní umožňuje i běžnou změnu hesla (bez resetu).	ACIdentita.pdf
	Individualizace	IDM umožní uživatelům individuálně nastavit vlastní zobrazení rozhraní - min. zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku - vždy pro každý seznam samostatně.	IDM umožňuje uživatelům individuálně nastavit vlastní zobrazení rozhraní včetně zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku - vždy pro každý seznam samostatně.	ACIdentita.pdf
	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.	IDM provádí zasílání konfigurovatelných emailových upozornění včetně následujících událostí: 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.	ACIdentita.pdf

	Šablony upozornění	Šablony upozornění umožní definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám musí být možné nastavovat různé příjemce pro různé části organizační struktury (např. třída, oddělení) apod. Šablony musí umožnit vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu.	Šablony upozornění umožní definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám je možné nastavovat různé příjemce pro různé části organizační struktury (např. odbor, oddělení) apod. Šablony umožňují vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu.	ACIdentita.pdf
	Bezpečnost změn	Veškeré změny vyvolané požadavky uživatele a administrátorů/správců IDM budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v identitách a referenčních objektech i v administraci a konfiguraci IDM. Záznam v logu bude obsahovat původní i novou hodnotu.	Všechny 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.	ACIdentita.pdf
	Důvěryhodnost	Veškeré požadavky na změny v IDM bude možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových soubory jako XML, CSV, atd. z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM.	Veškeré požadavky na změny v IDM bude možné zadávat výhradně prostřednictvím Portálu. Požadavky není možné realizovat ručními změnami textových soubory (XML, CSV atd.) z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM.	ACIdentita.pdf

	Auditní report	IDM umožní export auditního reportu z údajů o identitách uložených v IDM a to i historických. Auditní reporty budou minimálně ve formátu XML nebo CSV a budou obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IDM, pracovních pozic, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti. Filtrování reportovaných identit musí být možné podle libovolných atributů identity včetně přidružených referenčních objektů	IDM umožňuje export auditního reportu z údajů o identitách uložených v IDM a to i historických. Auditní reporty jsou ve formátu CSV a obsahují souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IDM, agendových rolí, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti.	ACIdentita.pdf
	Standardy WS	Systém bude disponovat aplikačním rozhraním (API) webových služeb, které budou definované v rozšířeném standardu WSDL a podporovat protokol SOAP.	Webové služby IDM jsou definované v rozšířeném standardu WSDL a podporují protokol SOAP.	ACIdentita.pdf
	Bezpečnost WS	Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně.	Konfigurace webových služeb umožňuje konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně.	ACIdentita.pdf
	Synchronizace	Ruční i automatické spuštění synchronizací s propojenými systémy. Musí být implementovány minimálně následující typy synchronizací: - Plná synchronizace – prochází všechny objekty v IDM a synchronizuje je s odpovídajícími objekty daného systému - Změnová synchronizace – synchronizuje jen změny od poslední provedené synchronizace. - Simulační synchronizace – synchronizace vytvoří report očekávaných změn v napojeném	Systém umožňuje ruční i automatické spuštění synchronizací s propojenými systémy. Systém umožňuje spuštění synchronizací i v simulačním režimu pro ověření dopadu reálného spuštění bez ovlivnění produkčních dat a napojených systémů. Simulační logy budou zobrazitelné v Portálu.	ACIdentita.pdf

		systému (bez ovlivnění produkčních dat). Průběh a výsledek všech synchronizací bude dostupný v přehledné podobě v grafickém prostředí Portálu	Zobrazení jednotlivých stavů průběhu synchronizace je k dispozici v přehledné grafické podobě.	
	Historie 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.	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.	ACIdentita.pdf
	Správa synchronizací	Veškerá správa jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, nastavení časového intervalu spouštění, nastavení intervalu odstávky a výběru synchronizované organizace bude součástí portálu.	Vestavěná správa jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, nastavení časového intervalu spouštění, nastavení intervalu odstávky. U jednotlivých synchronizací je možné vybírat organizace, které se mají z IDM	ACIdentita.pdf

			synchronizovat s danými systémy. Správa bude součástí Portálu.	
	Konektory	IDM bude spravovat identity a řídit oprávnění v dále vyjmenovaných systémech. V těchto systémech bude IDM vytvářet, aktualizovat, vytvářet uživatele, nastavovat jim oprávnění k rolím a (v prostředí cloudu) přiřazovat licence - Microsoft Active Directory - Microsoft 365 - obecný - simulace aplikace, požadavky na změny IDM zasílá e-mailem správci aplikce, který je jich provedení potvrzuje zpět v IDM pro účely evidence změn a logování - školský informační systém Bakaláři - ze systému budou načítány údaje o organizační struktuře, osobách a jejich vlastnostech a tyto údaje budou pro IDM sloužit jako zdrojové	IDM bude spravovat identity a řídit oprávnění v - Microsoft Active Directory - Google Workspace a/nebo Microsoft 365 V těchto systémech bude IDM vytvářet, aktualizovat, vytvářet uživatele, nastavovat jim oprávnění k rolím a (v prostředí cloudu) přiřazovat licence. Systém bude napojen na informační systém škola online	ACIdentita.pdf
	Záruka	60 měsíců včetně nároku na opravné verze	60 měsíců včetně nároku na opravné verze	Záruku poskytne dodavatel včetně zajištění přístupu k opravným verzím systému – služby jsou zahrnuty v nabídkové ceně.
Zálohování	Požadavky na licenci	Licence zálohovacího software pro nabízený hypervisor pro min. 15 zálohovaných virtuálních serverů, klientských stanic a neomezeného objemu dat.	Licence Veeam Data Platform Advanced v edici Essentials, obsahuje 15 univerzálních licencí umožňující zálohovat 15 virtuálních/fyzických serverů, až 45 stanic bez omezení objemu dat	veeam_data_platform_feature_comparison.pdf veeam_licensing_policy.pdf

	Požadavky na funkčnost	Integrované technologie komprimace a deduplikace.	Zálohovací řešení má integrovanou technologie komprimace a deduplikace.	veeam_data_platform_feature_comparison.pdf
		Provádění datově konzistentních záloh hlavních serverových aplikací – Microsoft SQL server, Active Directory, souborové systémy – bez nutnosti odstávky aplikace	Umožnuje provádění datově konzistentních záloh hlavních serverových aplikací – Microsoft SQL server, Active Directory, souborové systémy – bez nutnosti odstávky aplikace	veeam_data_platform_feature_comparison.pdf
		Software musí umožňovat v rámci jedné zálohovací úlohy ukládání souborů záloh do více fyzických diskových úložišť s různým typem připojení a od různých výrobců pro usnadnění škálovatelnosti řešení	Software umožňuje v rámci jedné zálohovací úlohy ukládání souborů záloh do více fyzických diskových úložišť s různým typem připojení a od různých výrobců pro usnadnění škálovatelnosti řešení	veeam_data_platform_feature_comparison.pdf
		Řešení musí podporovat granulární obnovu	Řešení musí podporuje tzv. granulární obnovu	veeam_data_platform_feature_comparison.pdf
		Řešení musí umožnit replikaci min. 15 virtuálních serverů mezi hypervisory	Řešení umožňuje replikaci 15 virtuálních serverů mezi hypervisory	veeam_data_platform_feature_comparison.pdf
		Řešení musí nativně podporovat nabízené bezpečné úložiště	Řešení nativně podporuje tzv. Veeam (Linux) Hardenned Repository	veeam_data_platform_feature_comparison.pdf
		Řešení musí poskytovat dohled nad chráněnou virtualizační platformou, poskytující včasná varování před výpadkem, nebo omezením dostupnosti produkčního prostředí	Licence Veeam Data Platform obsahuje monitoring virtualizační platformy Veeam ONE, který poskytuje dohled nad chráněnou virtualizační platformou, poskytuje včasná varování před výpadkem, nebo omezením dostupnosti produkčního prostředí.	veeam_data_platform_feature_comparison.pdf

		Řešení musí informovat, které VM nejsou chráněné dostatečně, nebo vůbec a zároveň kdy a jakým spůsobem byl naposledy vytvořen bod obnovy.	Licence Veeam Data Platform obsahuje monitoring virtualizační platformy Veeam ONE, který dokáže informovat, které VM nejsou chráněné dostatečně, nebo vůbec a zároveň kdy a jakým způsobem byl naposledy vytvořen bod obnovy.	veeam_data_platform_feature_comparison.pdf
		Řešení musí nabídnout inteligentní diagnostiku zálohovacího řešení sledováním protokolů o známých problémech a nesprávných konfiguracích a nabízením řešení bez otevírání požadavků na podporu výrobce, nebo odesílání diagnostických dat.	Řešení nabízí inteligentní diagnostiku zálohovacího řešení sledováním protokolů o známých problémech a nesprávných konfiguracích a nabízením řešení bez otevírání požadavků na podporu výrobce, nebo odesílání diagnostických dat.	veeam_data_platform_feature_comparison.pdf
		Řešení musí podporovat automatizované vytváření a zasílání reportů e-mailem	Řešení podporuje vytváření reportů a jejich zasílání emailem	veeam_data_platform_feature_comparison.pdf
		Řešení musí umožňovat pravidelné automatické testování obnovitelnosti záloh, včetně funkčnosi jednotlivých služeb a kontrolou obsahu na kybernetické hrozby (ransomware)	Řešení obsahuje funkci Sure Backup, která zajišťuje pravidelné automatické testování obnovitelnosti záloh, včetně funkčnosi jednotlivých služeb. Řešení dále umožňuje kontrolou obsahu na kybernetické hrozby (ransomware)	veeam_data_platform_feature_comparison.pdf
		Řešení musí umožňovat monitorování zatížení zálohovacího serveru, množství chráněných dat, stav zálohovacích úloh, stav replikačních úloh a stav kontrolních úloh obnovitelnosti VM	Řešení umožňuje monitorování zatížení zálohovacího serveru, množství chráněných dat, stav zálohovacích úloh, stav replikačních úloh a stav	veeam_data_platform_feature_comparison.pdf

			kontrolních úloh obnovitelnosti VM	
	Záruka	60 měsíců včetně nároku na opravné verze	Licence na 60 měsíců, včetně nároku na opravné verze	Součástí nabídkové ceny