TECHNICKÁ SPECIFIKACE

pro veřejnou zakázku malého rozsahu na služby s názvem

Služby v oblasti IT

Požadavky zadavatele:

1. **Služba zálohy a synchronizace v cloudovém úložišti**

   Nepřetržitý provoz 24/7, včetně podpory a monitoringu dostupnosti služby.

   Služba musí zajistit kapacitu minimálně 400 GB cloudového úložiště pro účely zálohy a synchronizace dat.

   Řešení musí podporovat víceuživatelské prostředí – správu uživatelských účtů s možností nastavení oprávnění a auditování přístupů.

   Musí umožňovat sdílení dat mezi jednotlivými uživateli ve skupinách i mezi skupinami s granularitou přístupových práv.

   Služba umožní synchronizaci cloudového uložiště s lokálními zařízeními (Windows, macOS, Linux, mobilní platformy), včetně automatizované obousměrné synchronizace vybraných složek a souborů.

   Přístup k zálohám, správě a synchronizaci dat musí být možný přes webové rozhraní i mobilní aplikaci (Android, iOS).

   Poskytovatel garantuje obnovu dat ze zálohy do 4 hodin od nahlášení incidentu (RTO ≤ 4 hodiny).

   Data musí být fyzicky uložena na území České republiky – poskytovatel je povinen doložit konkrétní lokalizaci datacentra.

   Cloudové služby musí splňovat nejvyšší bezpečnostní standardy (šifrování AES-256, anti-malware, ochrana před ransomwaru, auditovatelnost přístupů a historie změn).

   Služba umožňuje verzionování dokumentů, granularní obnovu jednotlivých souborů/složek i obnovu celého uživatelského prostoru.

   Musí být vyhověno zákonným a regulatorním požadavkům na ochranu osobních a citlivých dat v ČR.

2. **Provoz vysokokapacitního datového uložiště pro archivaci a práci s daty**

   Nepřetržitý provoz 24/7, včetně podpory a monitoringu dostupnosti služby.

   Systém musí umožňovat nastavení oprávnění a rolí pro jednotlivé uživatele a skupiny, přičemž správa přístupů musí být řízena doménovou politikou (Active Directory nebo obdobným řešením).

   Kapacitní škálovatelnost: Systém musí podporovat kapacitní růst úložiště dynamicky dle aktuálních a budoucích potřeb zadavatele bez výpadků provozu.

Lokalizace dat: Všechna data, včetně podkladů zastupitelstva a rady města, musí být fyzicky uložena na území České republiky v datových centrech splňujících certifikace a požadavky na bezpečnost.

Replikace a redundance: Data musí být replikována do geograficky oddělených lokalit pro zajištění vysoké dostupnosti a odolnosti proti výpadkům.

Retention (retence) dat: Možnost uchovávat a obnovovat data minimálně 7 dní zpětně dle nastavených retence politik.

Ochrana proti ransomwaru: Datové centrum a úložiště musí být „ransomware ready“ s implementací anti-malware technologií, monitoringem podezřelé aktivity a bezpečnostními protokoly proti ransomwarovým útokům.

Bezpečnost připojení: Komunikace s datovým úložištěm musí probíhat šifrovaným VPN spojení s certifikátem a dodržováním standardů šifrování.

Certifikace datového centra: Datová centra musí mít validované certifikace a audity, zejména:

ANSI-TIA942 (infrastruktura)

ISO/IEC 15408 (bezpečnostní standardy IT produktů)

CC EAL 4+ (evaluace bezpečnosti)

ISO 9001 (řízení kvality)

ISO 14001 (environmentální management)

ISO 19011 (auditování systémů řízení)

ISO/IEC 20000-1 (řízení IT služeb)

ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 (informační bezpečnost a cloudové služby)

ISO 50001 (řízení energie)

PCI-DSS (platby a zabezpečení dat karet)

NBÚ ČR pro stupeň utajení TAJNÉ (bezpečnostní požadavky státní správy)

GDPR (ochrana osobních údajů)

Smluvní závazky: Poskytovatel musí garantovat dodržení všech výše uvedených parametrů smluvně v souladu s platnou legislativou a SLA dle této specifikace.

Auditovatelnost: Možnost pravidelných auditů bezpečnosti, provozu a shody s certifikacemi z pohledu zadavatele.

Monitoring a hlášení: Real-time monitoring provozu s automatickým hlášením incidentů, s rychlým řešením incidentů a obnovou dat dle smluvených časů.

3. **Základní správa IT (budova radnice, budova pobočná, budova knihovna KD, budova DPS, prostory městské policie) paušál 5 hodin měsíčně**

   Požadované činnosti:

   Zajištění základní údržby a pravidelných aktualizací systémů VITA, Ginis, Gordic tak, aby byla zajištěna jejich provozní spolehlivost a bezpečnost.

   Správa a konfigurace prostředí JIP/KAAS včetně potřebné dokumentace a optimalizace výkonu.

   Správa uživatelů a certifikátů přes portál PostSignum.

   Obnova certifikátů, správa tokenů a čipových karet.

   Správa a konfigurace Hyper-V virtualizačního prostředí a virtuálních serverů se zachováním vysoké dostupnosti.

   Centrální správa antivirového systému ESET/EDR s pravidelnými aktualizacemi a monitoringem bezpečnostních hrozeb.

   Administrace a správa lokálního poštovního serveru Kerio Connect včetně zálohování a obnovy dat.

   Správa centrálního firewallu Kerio Control, včetně integrace s Active Directory pro řízení přístupových práv.

   Správa a údržba lokální Active Directory včetně uživatelské a bezpečnostní administrace.

   Správa a údržba tiskového a skenovacího softwaru FlowCAP s podporou uživatelských požadavků.

   Kontrola a správa zálohování dat, jak lokálního, tak cloudového, zahrnující pravidelné testy obnovitelnosti záloh.

   Centrální správa UNIFI ekosystému (Wi-Fi a síťových zařízení) zajišťující optimální pokrytí a bezpečnost.

   Servis PC, notebooků, mobilních zařízení (platformy Android a Apple) a serverů užívaných pracovníky úřadu a zastupitelstva.

   Správa aktivních síťových prvků značky DELL včetně konfigurace a monitoringu.

   Reakční doby:

   Požadovaná dostupnost osobní účasti na místě od nahlášení kritického incidentu: 2 hodiny.

   Požadovaná dostupnost vzdálené podpory od nahlášení incidentu, s možností okamžité diagnostiky a řešení problémů: 2 hodiny.

4. **Služby IT – instalace, konfigurace a aktualizace - paušál 50 hodin měsíčně**

   Dodavatel bude zajišťovat následující činnosti:
   Pravidelná instalace a konfigurace systémových a bezpečnostních aktualizací na Hypervisoru 2019 (včetně kontroly kompatibility virtualizovaného prostředí).

   Pravidelná instalace a konfigurace aktualizací operačních systémů a aplikačních komponent na virtuálním serveru VITA.

Pravidelná instalace a konfigurace aktualizací na virtuálním serveru určeném pro vysokokapacitní úložiště, využívaném k archivaci podkladů pro zastupitelstvo a radu města, včetně řízení přístupových práv a zálohování.

Pravidelná instalace a konfigurace systémových a aplikačních aktualizací na serveru GINIS s kontrolou závislostí a verze databází.

Pravidelná instalace a konfigurace aktualizací na VM Fileserver včetně kontroly integrity dat a stavu uložiště.

Instalace a konfigurace aktualizací na VM Micos a Unifi Controller, včetně správné funkčnosti Wi-Fi systémů a síťové infrastruktury.

Instalace a konfigurace aktualizací na VM Home and storage users, zajištění bezpečnosti a výkonu uživatelských uložišť.

Instalace a konfigurace aktualizací na VM Print and Scan, včetně podpory tiskových a skenovacích služeb dodavatele.

Instalace a konfigurace aktualizací na VM ESET Protect, včetně kontroly aktuálnosti antivirové databáze a funkčnosti centrální správy.

Instalace a konfigurace aktualizací na doménovém řadiči DCKD1, včetně správy politik a uživatelských rolí.

Instalace a konfigurace aktualizací na VM Terminal for users, optimalizace výkonu a dostupnosti služby pro koncové uživatele.

Pravidelná kontrola zálohování, včetně provádění testů obnovitelnosti záloh, kontroly stavu RAID, pročištění dočasných (TEMP) a logovacích (LOG) souborů.

Instalace systémových aktualizací a aplikačních patchů na VM Kerio Connect.

Pravidelná aktualizace poštovního serveru Kerio Connect včetně zálohování a obnovy dat.

Pravidelná aktualizace firmware na bezpečnostní bráně Kerio Control, včetně integrace nové verze do provozního prostředí a zachování kompatibility s Active Directory.

Reakční doby:

Požadovaná dostupnost osobní účasti na místě od nahlášení kritického incidentu: 2 hodiny.

Požadovaná dostupnost vzdálené podpory od nahlášení incidentu, s možností okamžité diagnostiky a řešení problémů: 2 hodiny.

5. Služby IT – uživatelská a technická podpora - paušál 30 hodin měsíčně

Řešení běžných dotazů a problémů, které se mohou vyskytnout:

Podpora při instalaci, odinstalaci a konfiguraci produktů v pracovním prostředí zákazníka.

Asistence s aktualizací, upgrade a správou licencí včetně řešení chyb během implementace nebo migrace systému.

Řešení problémů s připojením (sítě, VPN, porty, firewall), komunikace s veřejným internetem i interními systémy.

Nastavení a správa zabezpečení, pravidel (firewall, antimalware, EDR/XDR politiky), detekce a odstranění škodlivého softwaru, řešení incidentů a monitorování hrozeb.

Obslužné dotazy související s běžným provozem systému (změna hesla, správa účtů, obnova přístupu, export a archivace dat, reporty atd.).

Řešení problémů s aktualizacemi antivirových databází, nefunkčností rezidentní ochrany, nastavení výjimek a politik, řešení upozornění systému.

Export, sběr a analýza protokolů pro detailní diagnostiku neobvyklého chování nebo incidentů.

Odborné poradenství při zapojení nových zařízení, obnově po havárii, migraci na jinou platformu nebo při integraci s dalšími systémy.

Podpora při obnově a řešení blokovaných funkcí, včetně postupů "troubleshooting" a “incident response”.

Zaškolení uživatelů na běžnou obsluhu, základní správu systému a řešení nejčastějších situací.

Komunikace s dodavateli třetích stran (VITA, Gordic, CzechPoint, PostSignum).

6. Další služby

Internetová konektivita:
"Symetrické připojení s min. kapacitou dle specifikace:

1x 50Mbps symetrické připojení pro policii

1x 50Mbps symetrické připojení pro městskou knihovnu

1x optický spoj pro městský úřad

1x 50Mbps symetrické připojení pro DPS

Garantovaná dostupnost min. 99,5% ročně, agregace 1:1.

Transparentní reporting o provozu a monitoringu s reakcemi na incidenty do 4 hodin v pracovní době.

Ochrana připojení před kybernetickými hrozbami (antimalware, firewall, ochrana proti DoS/DDoS útokům).

SLA pokrývající reakční dobu a time-to-repair včetně technické podpory."

Hostingové služby
Provoz webhostingu pro rezervační systém a internetovou prezentaci na doméně www.hala-kd.cz s oddělenými nebo sdílenými servery podle požadavku zadavatele.

Garantovaná dostupnost hostingu min. 99,5% ročně; podpora HTTPS certifikace a pravidelné bezpečnostní aktualizace.

Pravidelné zálohování (min. 1x denně), obnova do 4 hodin, možnost testovaného disaster recovery scénáře.

Technická podpora a monitoring provozu, včetně pravidelného reportingu funkčnosti.

Doménové služby

Registrace, správa a provoz domény (hala-kd.cz), včetně řízení DNS záznamů.

Ochrana doménových údajů v souladu s GDPR a soulad s požadavky doménového registru.

Garance funkčnosti DNS infrastruktury a pravidelné kontroly.

VOIP infrastruktura

Poskytování a správa VOIP ústředny a telefonních služeb s měsíční fakturací.

SLA dostupnosti 24/7, reakční doba na incidenty max. 4 hodiny.

Zahrnuje dohled, správu licencí, aktualizace a reporting provozu i volání.

7. Licence

i. **Prodloužení platné licence pro firewallový systém Kerio Control na období 24 měsíců (2 roky) s kapacitou minimálně 25 současně připojených uživatelů. Licence musí umožňovat všechny funkce odpovídající kompletní verzi produktu (včetně aktualizací, podpory, centrální správy, bezpečnostních funkcí a logování provozu). Dodavatel doloží platnou licenci vystavenou výrobcem nebo autorizovaným distributorem, a to nejpozději v den zahájení plnění.**

   Obnova a zajištění kontinuity všech funkcí stávající instalace Kerio Control bez přerušení.

   Přístup k oficiálním aktualizacím a technické podpoře výrobce v celém rozsahu licencovaného období.

   Garance souladu s licenčními podmínkami výrobce na počet uživatelů a rozsah funkcí.

   Doložení licence/klíče v elektronické podobě.

ii. **Prodloužení platné licence Kerio Connect Maintenance na období 24 měsíců (2 roky) pro kapacitu 65 uživatelů. Součástí licence musí být aktivní rozšíření Kerio AntiSpam, Kerio AntiVirus a ActiveSync. Licence musí být vystavena výrobcem nebo autorizovaným distributorem a pokrývat pravidelné aktualizace, bezpečnostní opravy a přístup k technické podpoře výrobce v kompletním rozsahu po celou dobu plnění.**

   Zachování všech funkčností stávající instalace Kerio Connect bez přerušení. Přístup k oficiálním aktualizacím, včetně bezpečnostních a antivirových databází, a ochrany proti spamu.

   Garance souladu s licenčními podmínkami výrobce, včetně licence pro ActiveSync (mobilní synchronizace), AntiVirus a AntiSpam pro deklarovaný počet uživatelů. Doložení licence/klíče v elektronické podobě s jasným určením počtu uživatelů a aktivovaných rozšíření.

   Podpora multiplatformního přístupu (Outlook, mobilní zařízení, webové rozhraní) a možnost archivace a zálohování dat.

iii. **Dodání důvěryhodného komerčního SSL certifikátu typu Wildcard pro hlavní doménu a všechny její subdomény ve tvaru *.kraluv-dvur.cz, s platností na období 24 měsíců. Certifikát musí být uznáván všemi hlavními internetovými prohlížeči a umožnit zabezpečenou HTTPS komunikaci napříč subdoménami včetně hlavního webu kraluv-dvur.cz.**

Certifikát vystavený certifikační autoritou plně uznávanou hlavními prohlížeči (CA s globální důvěryhodností).

Platnost certifikátu minimálně 365 dní.

Možnost využití pro neomezený počet subdomén (Wildcard forma *.kraluv-dvur.cz), včetně hlavní domény kraluv-dvur.cz.

Vydání certifikátu na základě OV validace (ověření organizace), případně DV validace (ověření domény) dle nabídky zadavatele.

Nastavení a předání kompletní dokumentace a klíčových materiálů (private key, public key, intermediární certifikáty, instalační postup).

Podpora při nasazení certifikátu a validace správné implementace v produkčním prostředí.

Garance zajištění pravidelných aktuálních CRL a OCSP pro bezproblémové ověřování platnosti.

Zajištění možnosti rychlého zrušení a opětovného vystavení v případě incidentu (např. kompromitace klíče).

Podpora technické asistence po celou dobu platnosti certifikátu.

iv. **Dokoupení licence k softwaru Micos RS 2025 s oprávněním k provozu na 30 pracovních stanicích (PC). Licenční plnění musí být v souladu s aktuálními podmínkami výrobce, zahrnovat plnou funkčnost produktu, nárok na aktualizace v rámci zakoupené verze a možnost technické podpory ze strany dodavatele po dobu minimálně 24 měsíců od aktivace. Dodavatel je povinen doložit platnou licenci/klíč, ve formě certifikátu nebo elektronického dokladu.**

Zajištění aktivace nebo rozšíření současného licenčního poolu na 30 pracovních míst. Přístup k oficiálním aktualizacím a opravám softwaru pro verzi 2025 po celou dobu licence.

Technická podpora pro správce IT a uživatele v rámci délky licenčního vztahu.

Doložení licenčních práv pro zadavatele.

v. **Prodloužení platné licence pro bezpečnostní řešení ESET PROTECT ELITE s platností na 24 měsíců (2 roky), pro 50 pracovní stanic (PC, notebooky, servery). Licence musí zahrnovat komplexní ochranu koncových zařízení, vzdálenou správu přes ESET PROTECT On-Prem Web Console, právo na pravidelné produktové a**

antivirové aktualizace, technickou podporu a přístup k výrobci v celém období prodloužené licence.

Licence pro 50 zařízení na dobu 2 let, vystavená výrobcem či autorizovaným distributorem.

Pokrytí produktů ESET Endpoint Security, ESET Endpoint Antivirus a ochranu firemních serverů v souladu s podmínkami produktu Essential On-Prem.

Možnost centrálního managementu a konfigurace bezpečnostních politik přes webové rozhraní.

Pravidelné bezpečnostní a antivirové aktualizace, včetně automatické distribuce na všechny zařízení.

Podpora reinstalace/aktivace licence při upgrade či výměně HW. Zajištění technické podpory po dobu trvání licence a možnost obnovení/řešení incidentu s výrobcem.

Elektronické doložení licence/klíče pro zadavatele, automatizovaný reporting stavu ochrany.

vi. **Dodávka potřebného počtu licencí (50) řešení EDR, včetně jejich implementace, aktivace, centralizované správy a technické podpory na dobu 24 měsíců.**

Poskytnutí platné licence ESET EDR vystavené výrobcem nebo autorizovaným distributorem s možností centrální správy a remote managementu přes webové rozhraní (ESET PROTECT nebo Inspect).

Implementace řešení v prostředí objednatele, včetně nasazení agentů na cílová zařízení, vytvoření základních bezpečnostních politik, a zajištění plné provozní funkčnosti systému EDR.

Zajištění detekce, analýzy a reakce na bezpečnostní incidenty na koncových bodech a serverech včetně nástrojů pro sběr, korelaci a vyhodnocení podezřelé aktivity.

Pravidelné aktualizace systému, threat intelligence, detekčních pravidel a funkcionalit EDR dle výrobce.

Zaškolení administrátorů objednatele na správu a základní údržbu systému minimálně v rozsahu 2 hodin.

Technická podpora přes e-mail, telefon a web formu v režimu minimálně 8x5 po celou délku smluvního vztahu s možností rozšíření na vyšší SLA dle nabídky.

Doložení licenčních klíčů, potřebné dokumentace a případně instalačních balíčků.