

Příloha č. 6 – Výzvy k podání nabídky

TECHNICKÁ ČÁST ZADÁVACÍ DOKUMENTACE

k veřejné zakázce

„Expertní podpora infrastruktury informačního systému KÚ“

## Obsah

Vymezení předmětu zakázky .....	- 3 -
Podrobné členění .....	- 3 -
Správa a podpora IS.....	- 3 -
Podporované systémy a aplikace .....	- 3 -
Specifikace služeb.....	- 3 -
Profylaktické činnosti všech podporovaných systémů.....	- 4 -
Kvalifikace.....	- 5 -
Seznam významných zakázek .....	- 5 -
Způsob zajištění služby .....	- 5 -
Požadavky na kvalitu technického (expertního) týmu: .....	- 6 -
Součinnost Zadavatele .....	- 6 -
Zpracování dokumentace .....	- 6 -

## Vymezení předmětu zakázky

Zadavatel (Středočeský kraj) požaduje zajištění externích služeb týkající se správy a podpory aplikační a technologické infrastruktury informačního systému krajského úřadu „IS KÚ“ (dále jen systémová podpora).

## Podrobné členění

### Správa a podpora IS

Čerpání služeb bude řešeno na základě aktuální potřeby Odboru informatiky, a to vždy dílčími požadavky, které budou schváleny vedoucím odboru či jeho zástupcem, popř. administrátorem sítě IS KÚ. Zadavatel předpokládá zajištění externích služeb v rozsahu 4 dnů v týdnu (PO-ČT), tj. fyzickou přítomnost administrátora (s předpokladem okamžitého zastoupení) a součinnost s interním administrátorem na aktuálních úkolech a projektech v oblasti ICT a bezpečnosti. Podpora externích služeb bude dále zahrnovat vzdálenou správu prostřednictvím VPN a externí řešení IT požadavků. Zadavatel dále požaduje účast na technických schůzkách, zejména v oblasti rozvoje IS KÚ a bezpečnosti. Celkový rozsah je 200 MD (12 měsíců) za dobu účinnosti smlouvy, přičemž 190 MD bude průběžně čerpáno na expertní podporu (Microsoft) a 10 MD na expertní podporu (Fortinet).

Zadavatel dále předpokládá, že základní rekognoskace a úvodní seznámení s IS KÚ vč. předání dokumentace bude součástí výše uvedených 190 MD.

Administrace IS bude zahrnovat tyto oblasti:

### Podporované systémy a aplikace

Systémová podpora bude koncentrovaná na následující produkty:

- Microsoft Windows Server
- Microsoft Exchange Server
- Microsoft SQL Server
- Microsoft SharePoint Foundation/Server
- Monitorovací a konfigurační serverové systémy Microsoft
- MS služby ADDS, ADFS, ADCS, DHCP, FSS, PDS, WAP, SUS, VAS, WEB (IIS), WDS včetně spojených infrastrukturních služeb
- Antivirová ochrana koncových bodů Symantec Endpoint Protection
- Antivirová a antispamová ochrana SMTP provozu Symantec Message Gateway
- Services M365 (komplexní správa Tenant)
- Cloud Services Microsoft Azure
- VMware, vCenter – dohled

Systémová podpora v rozsahu daném touto zadávací dokumentací se vztahuje i na nové verze podporovaných produktů a systémových komponent.

### Specifikace služeb

Poskytovatel se zavazuje na základě této Smlouvy pro Objednatele provádět tyto služby a dodávky související s činností Objednatele:

- poskytování služeb kontaktního místa,
- profylaktické činnosti podporovaných systémů,
- řešení havarijních stavů, incidentů, problémů a požadavků na místě nebo vzdáleně,
- dílčí projektová a architektonická činnost v oblasti ICT,

- prediktivní rozvoj Microsoft infrastruktury v místě plnění zakázky,
- nasazení automatizovaných procesů za využití MS konfiguračních a monitorovacích systémů,
- zajištění integrace současné infrastruktury do prostředí M365 E3 s přesahem do E5,
- účast na technických a konzultačních schůzkách týkají se rozvojových projektů v oblasti ICT, a projektů v oblasti bezpečnosti IS.

## Profylaktické činnosti všech podporovaných systémů

Služby profylaktické činnosti zahrnují následující aktivity pro podporované systémy Microsoft:

- instalace, reinstalace, upgrade, implementace opravných balíků a záplat (ServicePacks, Patches),
- zabezpečení systémových požadavků a jednotného prostředí pro další systémy,
- kontrola hlavních výkonnostních parametrů systému a návrhy na případné změny,
- pravidelná analýza událostí uložených v systémovém logu a následné odstranění problémových stavů,
- pravidelná analýza událostí uložených v aplikačním logu a následné vyvození příslušných opatření vedoucích k větší stabilitě provozovaných aplikací,
- pravidelná kontrola základních konfiguračních parametrů a nastavení jednotlivých instalovaných systémů a komponent,
- pravidelná profylaxe fyzických a virtuálních serverů (VMware) – s instalovanými MS produkty,
- dohled a profylaxe systémů, které jsou umístěny v technologickém centru Praha a Kladno.

Dále služby v oblasti bezpečnosti konkrétních produktů společnosti Fortinet:

- vyhodnocování a revize provozu bezpečnostních technologií (FW, Sandbox, Analyzer, Mail),
- spolupráce s Odborem informatiky a Odborem bezpečnosti a krizového řízení na revizích bezpečnostních pravidel,
- spolupráce v oblasti přípravy procesních, provozních a bezpečnostních dokumentů.

Oblasti definované touto technickou zadávací dokumentací budou vykonávány v součinnosti s administrátorem sítě IS KÚ, tj. jde o tzv. doplňkové služby. Zadavatel v tomto směru nepředpokládá plné/výhradní převzetí systémové podpory dodavatelem, avšak očekává řešení systémové podpory v kooperaci s interním administrátorem IS vč. zajištění plnohodnotného zástupu (dovolená, pracovní volno apod.).

**Služby systémové podpory budou poskytovány v místě určeném Zadavatelem, a to buď prostřednictvím technika podpory Dodavatele na místě plnění (Středočeský kraj, Zborovská 11, 150 21 Praha 5) nebo vzdáleně, prostřednictvím VPN (RDP).**

**Služby budou poskytovány v pracovní dny, zejména PO-ČT v době od 8 do 17 hodin. Služby nebudou primárně poskytovány ve dnech pracovního volna, ve dnech pracovního klidu a o státních svátcích, které platí na území ČR, pokud se tak předem Zadavatel nedohodne s dodavatelem v rámci těchto případů: systémový zásah, výpadky systému, plánované a neplánované odstávky, řešení bezpečnosti, výpadky technologických lokalit.**

Služby technické podpory jsou poskytovány na řádně zakoupených licencích Zadavatele a infrastrukturu, která je ve správě Odboru informatiky.

## Kvalifikace

### Seznam významných zakázek

Uchazeč uvede alespoň 2 významné zakázky (oblast poskytování služeb – veřejná správa), poskytnuté za poslední 3 roky před zahájením výběrového řízení, včetně uvedení ceny a doby jejich poskytnutí a identifikace kontaktní osoby objednatele (**reference nebudou obsahovat konkrétní referenci zadavatele!!!**). Za významnou zakázku se považuje služba s obdobným předmětem plnění, tj. zajištění správy a podpory aplikační a technologické infrastruktury informačních systémů, a která má současně tento rozsah stanovených služeb:

- zajištění podpory on-site na místě objednatele v min. rozsahu 2MD/týdně
- zajištění podpory pro tyto systémy:
  - Microsoft Windows Server,
  - MS služby ADDS, ADFS, ADCS, DHCP, FSS, PDS, WAP, SUS, VAS, WEB (IIS), WDS včetně spojených infrastrukturních služeb,
  - Microsoft Exchange Server,
  - Microsoft SQL Server,
  - Microsoft SharePoint,
  - Monitorovací a konfigurační serverové systémy Microsoft,
  - Antivirová ochrana koncových bodů Symantec Endpoint Protection,
  - Antivirová a antispamová ochrana SMTP provozu Symantec Message Gateway,
  - Services M365 (komplexní správa Tenant),
  - Cloud Services Microsoft Azure,
  - VMware, vCenter – dohled,
  - provoz bezpečnostních technologií (FW, Sandbox, Analyzer, Mail Gate od společnosti Fortinet).
- hodnota každé ze zakázek – minimálně 780 000,-Kč bez DPH s rozlišením 1 zakázka na podporu systémů Microsoft a 1 zakázka na podporu systémů Fortinet (bezpečnost).

Seznam uvedených zakázek musí přesně odpovídat výše uvedeným službám v oblasti podpory systémů Microsoft, Fortinet a musí dále obsahovat aktuální kontakty (tel. a email) na referenční osoby z důvodu ověření rozsahu poskytovaných služeb u jiných zákazníků/subjektů.

**Pokud dodavatel neuvede v rámci významných zakázek služby, ze kterých nebude zřejmé, že uvedené oblasti v posledních 3 letech realizoval, bude vyloučen z dalšího hodnocení.**

### Způsob zajištění služby

Zadavatel požaduje, aby výše popsany předmět plnění byl zajišťován **odborně způsobilým dodavatelem a jeho techniky, kteří mají odborné znalosti a zkušenosti, a to alespoň v rozsahu:**

- alespoň dvěma techniky s kompetencemi:
  - Microsoft® Certified Solutions Expert: Cloud Platform and Infrastructure,
  - MCSE – Microsoft Certified Solutions Expert (MCSA: Windows Server 2012),
  - minimální odborná kvalifikace – délka praxe minimálně 10 let.
- alespoň jedním technikem s odbornou znalostí produktů Fortinet s tímto certifikátem:
  - NSE 8 Certification

Zadavatel požaduje, aby součástí nabídky byly životopisy expertního týmu, tj. jednotlivých techniků, které budou obsahovat odbornou praxi a zároveň projekty, na kterých se jednotliví členové týmu podíleli.

Pokud dodavatel neuvede do své nabídky výše uvedené životopisy a certifikaci, bude vyloučen z dalšího hodnocení.

Požadavky na kvalitu technického (expertního) týmu:

Vzhledem k tomu, že se jedná o systémovou podporu IS KÚ, zadavatel technickému týmu předloží 10 otázek dle výše specifikovaných služeb, aby ověřil technické znalosti jednotlivých expertů. Otázky budou vypracovány písemně s následným ústním projednáním. Každá otázka bude hodnocena 1 bodem. Písemné otázky a jejich vyhodnocení budou součástí protokolu o vyhodnocení veřejné zakázky.

Zadavatel důrazně připomíná, že tato zakázka je zadávána mimo režim zákona, jako zakázka malého rozsahu „VZMR“ tj. zadavatel si vyhrazuje právo stanovit podrobnější a přísnější kvalifikační kritéria pro posouzení kvality technického týmu.

Pokud v písemném testu nezíská technický tým min. 8 bodů, bude dodavatel z dalšího hodnocení vyloučen. Přesný termín písemného testu bude sdělen jednotlivým uchazečům na kontaktní email, který bude uveden na krycím listu. Na vypracování testu bude mít technický tým max. 20 minut.

### Součinnost Zadavatele

Zadavatel se zavazuje umožnit dodavateli přístup k podporovanému systému a poskytnout mu veškeré informace a potřebnou součinnost k provádění „Služeb systémové podpory“ vč. předání úvodní dokumentace a rekognoskace prostředí IS KÚ.

### Zpracování dokumentace

Zadavatel dále požaduje, aby dodavatel průběžně v rámci systémové podpory zajišťoval aktualizaci provozní a administrátorské dokumentace, zejména pak správu a údržbu konfigurační databáze, která je vedena v provozním systému úřadu a provozních dokumentech „požadavky na infrastrukturu“, kde jsou primárně vedeny informace o aplikační a technologické infrastruktuře v rozsahu:

- Popis řešení
- Návrh řešení
- Požadavky na infrastrukturu (aplikační a databázová infrastruktura vč. sizingu)
- Schéma komunikace

Prostupy:

Jméno aplikace / systému/ databáze	směr provozu	zdroj/cíl	Aplikační protokol	porty	protokol TCP/IP	charakter provozu

- Správa systému
- Dostupnost
- Zálohování
  - Požadavky na zálohování aplikačních serverů
  - Požadavky na zálohování DB
- Obecné požadavky
  - Zřízení účtů
  - Profylaxe a monitoring

- Administrace
- Kontaktní matice
- Konceptuální model – schéma