Zadávací dokumentace

k veřejné zakázce s názvem

„Zajištění služby Security Operation Center (SOC)“

podlimitní veřejná zakázka na dodávky zadaná formou zjednodušeného podlimitního řízení dle § 38 zákona č.137/2006 Sb., o veřejných zakázkách, v platném znění (dále jen "zákon")

(dále jen „veřejná zakázka“ nebo „VZ“)

# Informace o zadavateli

Název zadavatele: Vodovody a kanalizace Pardubice, a.s.

Právní forma: 121‐akciová společnost

sídlo zadavatele: Pardubice ‐ Zelené předměstí, Teplého 2014, PSČ 530 02

zápis v OR: OR vedený Krajským soudem v Hradci Králové, oddíl B, vložka 999

IČ zadavatele: 60108631

DIČ: CZ60108631

adresa profilu zadavatele https://zakazky.vakpce.cz/

# Název veřejné zakázky

Název veřejné zakázky: Zajištění služby Security Operation Center (SOC)

# Druh zadávacího řízení

Tato veřejná zakázka je zadávána zadavatelem mimo režim zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, (dále jen „zákon“) jako veřejná zakázka malého rozsahu na služby (dále také „VZ“). Veřejná zakázka je zadávána v režimu uzavřené výzvy.

# Vymezení předmětu plnění veřejné zakázky

## Předmět zakázky

Předmětem zakázky jsou služby SOC, které musí představovat komplexní, efektivní a proaktivní ochranu síťových prostředích organizace a v průmyslových řídicích sítích (SCADA) Zadavatele. Služba SOC musí být provozována vysoce kvalifikovanými specialisty s dlouholetými zkušenostmi, kteří musí řešit kybernetickou bezpečnost v souladu s platnými právními normami. Pro analýzu bezpečnostní situace musí být využíván jak neustálý dohled nad korelovanými událostmi v centrálním prvku SOC pracoviště, tak i periodické analýzy přímo v nástrojích u zákazníka, a to skrze VPN připojení. Cílem řešení musí být pomoc organizaci zefektivnit práci s ICT systémy, šetřit čas strávený s hledáním a analýzou příčiny vzniklých bezpečnostních incidentů, což zamezí škodám způsobeným výpadkem provozu ICT služeb, možné ztrátě důvěrných dat a omezení provozu základní služby Zadavatele.

## Předpokládaná hodnota veřejné zakázky

Předpokládaná hodnota veřejné zakázky činí 2.999 999, - Kč bez DPH. Financování předmětu veřejné zakázky je zajištěno z vlastních zdrojů zadavatele.

## Doba plnění

Smlouva bude uzavřena na dobu určitou, do 31.12.2025,

## Místo plnění

Místem plnění je sídlo zadavatele.

# Rozsah služby SOC

**Hlavní oblasti služby SOC jsou následující:**

* Dodavatel musí v rámci poskytovaných služeb SOC používat nástroj GREYCORTEX MENDEL, případně srovnatelné eventuality pro monitoring a vyhodnocování SCADA sítě.
* Dodavatel zahrne bezpečnostní a provozní nástroje Zadavatele do systému monitoringu a vyhodnocování.
* Dodavatel musí provádět dohled nad interními sítěmi Zadavatele, v režimu 24/7.
* Dodavatel musí pravidelně provádět testování zranitelností.
* Dodavatel musí provádět detekci vzniklých událostí,
* analýzu detekovaných událostí,
* včasnou reakci na vyhodnocené události, alarmy a incidenty,
* pravidelný a srozumitelný reporting o bezpečnostní situaci a provozní kondici ICT systémů v síti.
* Dodavatel musí být schopen zajistit prevenci a aktivní reakce na případné kybernetické incidenty.

**Segmenty interních sítí Zadavatele:**

* Administrativní (dále jen AS)
* SCADA (dále jen SC)
* Záloha (dále jen ZA)

**Počet lokalit, které je nutné monitorovat a vyhodnocovat:**

Specifikace druhů lokalit je následující:

* Centrála (dále jen CE)
* Úpravna vody (dále jen ÚV)
* Čističky odpadních vod (dále jen ČOV)
* Administrativní kancelář (dále jen AK)

Velikost lokalit je specifikována přibližným počtem IP adres – počtem aktiv a toto číslo je dále uváděno v závorce.

* Centrála (CE), počtem IP adres (400), segmenty (AS), (SC), (ZA)
* Holice (AK), počtem IP adres (8), segmenty (AS)
* Přelouč (AK), počtem IP adres (8), segmenty (AS)
* Mokošín (ÚV), počtem IP adres (50), segmenty (AS), (SC)
* Hrobice (ÚV), počtem IP adres (70), segmenty (AS), (SC)
* Studená voda (ÚV), počtem IP adres (25), segmenty (AS), (SC) – zatím v realizaci
* Holice (ČOV), počtem IP adres (20), segmenty (AS), (SC)
* Přelouč (ČOV), počtem IP adres (5), segmenty (AS), (SC) – zde není core switch
* Dašice (ČOV), počtem IP adres (12), segmenty (AS), (SC)
* Chvaletice (ČOV), počtem IP adres (20), segmenty (AS), (SC)
* Rybitví (ČOV), počtem IP adres (120), segmenty (AS), (SC)

**Propojení lokalit:**

Propojení jednotlivých lokalit je realizováno technologií Fortinet FortiGate:

* Centrála – FG-200F-A
* Ostatní lokality – FG-60F

**Konsolidace perimetru:**

Přístup do internetu je konsolidován na FG v centrále Zadavatele a v ostatních lokalitách je přístup omezen jen na výjimky pro havarijní případy.

## Nástroj GREYCORTEX MENDEL + XDR(EDR)

Zadavatel požaduje dodávku nástroje GREYCORTEX MENDEL, případně srovnatelné alternativy dle technické specifikace, která je detailním způsobem popsána v příloze číslo 1. tohoto dokumentu.

## Bezpečnostní a provozní nástroje Zadavatele

Zadavatel požaduje zahrnutí bezpečnostních a provozních nástrojů Zadavatele do systému monitoringu a vyhodnocování. Jedná se o následující nástroje:

* Logmanager LOGM-16TB-D-G4
* Progress Flowmon
* Zabbix

## Dohled nad interní sítí a to včetně SCADA

Zadavatel požaduje dohled nad specifikovanými aktivy, monitoring a analýzu síťového provozu, odhalování aktivity hackerů včetně dalších pokročilých hrozeb, identifikaci rizika kybernetické bezpečnosti obecně - včetně špionáže, úniků dat, anomálií v chování, škodlivých aktivit zaměstnanců a dalších obtížně odhalitelných hrozeb.

## Testování zranitelností

Zadavatel požaduje pravidelné testování zranitelností u specifikovaných aktiv ve vnitřních síťových prostředích organizace a v průmyslových řídicích sítích (SCADA) Zadavatele a u specifikovaných aktiv dostupných z internetu.

## Detekci vzniklých událostí

Zadavatel el požaduje, aby pro detekci vzniklých kybernetických bezpečnostních událostí bylo prováděno:

* Detailní sběr a zpracování statistik o síťovém provozu na úrovni celé sítě, jednotlivých podsíti, všech hostů v síti a služeb na každém hostu. To vše libovolně kombinovatelné, včetně směrů provozu a umístění služeb.
* Možnost sběru informací z NetFlow sond na základě uživatelské konfigurace.
* Schopnost detekce nežádoucích vzorů chování na síti (útoky, anomálie datového provozu, nežádoucí aplikace, detekce virů a botnetů ve vnitřní síti, detekce odchozího spamu, provozních problémů).
* Detekce anomálií vzhledem k dlouhodobému profilu chování zařízení na síti na základě dynamického modelování endpointů - metoda EDM.
* Nastavení předdefinované sady pravidel pro odhalování obecných anomálií v síti, včetně možnosti uživatelem definovaných pravidel.
* Vyhodnocování na základě implementace standardu Bidirectional flows (RFC 5103).
* Okamžitá integrace informací ze služeb DNS, DHCP, DC, Threat Intelligence, WHOIS a geo-lokační služby.

## Analýza detekovaných událostí

Objednatel požaduje analýzu detekovaných kybernetických bezpečnostních událostí především v těchto oblastech:

### Detekce neznámých a cílených útoků a hrozeb

|  |  |
| --- | --- |
| Typy útoků a hrozeb | Metoda |
| Pokročilé neznámé útoky   * útoky na uživatelské účty * komunikace s botnetem * úniky dat * obecně anomální chování uživatelů a zařízení | ***Prediktivní analýza =*** detekce anomálií na základě změny automaticky naučeného chování na různých úrovních monitorované sítě. Jedná se o odchylky od normálu na úrovni sítě, podsítě, daného zařízení a aktivních služeb na daném zařízení. |
| Cílené hrozby   * RAT - Remote Access Trojan * APT – Advanced Persistent Threat * AVT – Advanced Volatile Threat | ***Detekce strojového chování =*** odlišení projevů malware od lidské legitimní komunikace prostřednictvím periodických vzorů chování |

### Detekce známých útoků a hrozeb

|  |  |
| --- | --- |
| Typy útoků a hrozeb | Metoda |
| Známé projevy škodlivého chování   * skenování sítě a zařízení * enumerace dat * detekce hádání hesel * DoS a DDoS útoky apod. | Behaviorální detekce na úrovni toků za pomoci pravidel pro detekci očekávatelných projevů útoků. |
| Známé hrozby a dříve popsané útoky   * malware pro běžná zařízení * malware pro mobilní zařízení * trojské koně * útoky na aplikační a DB servery * zranitelnosti na straně klientských aplikací (JAVA, Flash, MS Office, prohlížeče…) * aktuální hrozby – phishing, trojans, … * komunikace s blacklistovanými zařízeními (IP adresa, doména) | Detekce známých útoků na základě denně aktualizované *sady detekčních pravidel* (přes 40.000) a blacklistů (60.000 až 100.000 záznamů).  Příklady detekčních kategorií:  Attack Response, Botcc, Chat, Current Events, DNS, DOS, Exploit, File, FTP, Games, ICMP, IMAP, Malware, Mobile Malware, Netbios, POP3, P2P, Policy, RPC, SCADA, Scan, Shellcode, SQL, TELNET, TFTP, TLS-Events, TOR, Trojans, User Agents, VOIP, Web Client, Web Server, Worms. |

### Ověření s bezpečnostními zásadami a politikami

|  |  |
| --- | --- |
| Příklady nálezů | Ověřované politiky |
| Porušení vybraných politik pro ochranu dat GDPR   * využívání dat nepovolenými osobami/způsoby * rizika úniku osobních údajů | Ověření souladu identifikovaných komunikací a komunikačních vektorů obsahujících osobní údaje s předem definovanými politikami pro ochranu dat. |
| Porušení komunikační politiky   * Nedostupné služby a zařízení * Vznik nových nepovolených služeb a zařízení * Nepovolené komunikační vektory | Kontrola povolených a zakázaných služeb, prostupů a sítových politik – srovnání pozorované komunikační matice a uživatelem definovaných politik. |
| Porušení bezpečnostních politik   * používání anonymizačních (Tor) a P2P sítí * hraní her a používání nepovolených aplikací * prověrka šifrované komunikace * nepovolené DNS servery * tunelovaný DNS provoz * používání zranitelných a zastaralých aplikací apod. | Zásady dobré praxe v síťové bezpečnosti |

### Výkonnost sítě a aplikací

|  |  |
| --- | --- |
| Příklady měřených veličin | Monitorovaná oblast |
| NPM – Network Performance Monitoring   * objem a rychlost přenesených dat, síťových toků a paketů * počet komunikačních partnerů, aktivních hostů, ... | Výkonost sítě na úrovni celé sítě, jednotlivých podsítí, hostů a na nich běžících službách. |
| APM – Application Performance Monitoring   * rychlost přenosu dat na síti * rychlost aplikační odezvy | Rychlost odezvy aplikací měřitelných na síti vč. automatické detekce anomálií |

### Vizualizace sítě a forenzní analýza

|  |  |
| --- | --- |
| Příklady využití | Monitorovaná oblast |
| Filtrování a zobrazení libovolných dat v reálném čase dle potřeb uživatele např.:   * kdo s kým, kdy, jak komunikuje (komunikační partneři) * bezpečnostní incidenty vč. příslušných síťových toků a případně obsahu zachycených škodlivých paketů * využívané síťové služby vč. aplikačních metadat * komunikace uživatelem vybraných zařízení * výkonost aplikací a sítě apod. | Kompletní viditelnost na úrovni síťových toků: celá síť, podsítě, zařízení/hosti, služby (na všech síťových portech) vč. škodlivých payloadů  Příklady parametrů pro filtrování:  IP address, Host name , MAC address, Subnet , User name, Domain string, Service location, Traffic direction, Port, Protocol, Tunneled traffic, VLAN ID , Event, Event category, Incident status |
| Viditelnost proxy | Zobrazení cílových IP adres komunikace od zdrojových hostů na základě X-Forwarding-for |
| Rychlá analýza příčin a následků v reálném čase | Viditelnost do aplikačních metadat komunikačních protokolů  Příklady protokolů:  DNS, HTTP, HTTPS, TLS, MODBUS, SMB, SMB2, SSH, SSL, SMTP, FTP, DCERPC IRC, VNC, POP3, Oscar, SIP, MS-SQL DHCP |
| Jednoduché vyšetřování incidentů – bezpečnostních i provozních | Informace pro forenzní analýzu – bohatá metadata o síťovém provozu uchovávaná po požadovanou dobu (v řádu měsíců) |
| Záznam vybrané podezřelé komunikace pro analýzu | Volitelný záznam provozu (on-deman full packet capture) dle zařízení, komunikačního partnera, portu/služby, času atd. |

## Včasná reakce na vyhodnocené události, alarmy a incidenty

Zadavatel požaduje nepřetržité plnění provozních bezpečnostních rolí SOC. Jedná se především o operátory, specialisty a analytiky, kteří by se starali o správnou funkčnost bezpečnostních nástrojů a bezpečnost sítí nepřetržitě 24 hodin 7 dní v týdnu.

## Zadavatel požaduje SLA v minimálních hodnotách hlavních parametrů

* Provozní dostupnost senzorické infrastruktury SOC - 99,5%
* Dostupnost systémů monitoringu SOC – v režimu 24x7 (24 hodin denně, 7 dnů v týdnu)
* Dostupnost Operátorů SOC – v režimu 24x7 (24 hodin denně, 7 dnů v týdnu)
* Dostupnost CSIRT SOC – v režimu 24x7 (24 hodin denně, 7 dnů v týdnu)
* Vyhodnocení a analýza detekcí – v režimu 8x5 (8 hodin denně, 5 dnů v týdnu)
* Pohotovost Specialistů – mimo uvedenou pracovní dobu jsou specialisté k dispozici v pohotovostním režimu 24x7 (24 hodin denně, 7 dnů v týdnu)
* Čas detekce – 15 minut
* Čas kategorizace – 30 minut
* Čas reakce a eskalace – 60 minut
* SLA procesních vstupů a výstupů na straně dodavatele a zadavatele budou přesně specifikovány ve smlouvě.

## Proaktivní zásah

Zadavatel požaduje od dodavatele provedení nezbytného proaktivního zásahu pro případy detekce kybernetických bezpečnostních incidentů v kategorii III, dle VKB. Detailní procesní postup proaktivního zásahu dodavatele bude přesně specifikován ve smlouvě.

## Pravidelný a srozumitelný reporting

Zadavatel požaduje pravidelné měsíční reportování a osobní projednání reportu s přiděleným primárním specialistou Dodavatele.

# Legislativní povinnost

Organizace je osobou povinnou dle zákona č. 181/2014 Sb., zákon o kybernetické bezpečnosti (dále jen ZKB) a vyhlášky č. 82/2018 Sb., vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen VKB), je jako provozovatel základní služby povinná plnit povinnosti identifikace kybernetických bezpečnostních událostí a jejich následné vyhodnocení, zda se jedná o kybernetický bezpečnostní incident.

Po příchodu nového zákona o kybernetické bezpečnosti, který se předpokládá nejpozději v říjnu roku 2024, se zadavatel pravděpodobně stane poskytovatelem dvou regulovaných služeb, pitná voda a odpadní voda.

# Dodavatel

Zadavatel bude Dodavatele identifikovat jako významného dodavatele dle VKB a bude požadovat plnění následujících smluvních požadavků:

* plnění pravidel pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací, dle VKB § 8, odstavec (1), písmeno a).
* povinnost dodavatele dodržovat bezpečnostní politiky povinné osoby a jejich odsouhlasení dle přílohy č. 7 k vyhlášce č. 82/2018 Sb., písmeno f).
* dodržovat způsoby a úrovně realizace bezpečnostních opatření a určit obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření dle VKB, § 8, odstavec (2), písmeno b).
* v rámci uzavírané smlouvy VKB., § 8, odstavec (1), písmeno f), relevantní oblasti uvedené v příloze č. 7, VKB.

# Součinnost při plnění

Při spolupráci s Dodavatelem služby SOC musí probíhat vytěžování následujících dat a informací:

* Log dat z provozovaných systémů a bezpečnostních nástrojů – cílem je sběr informací o kondici systémů a aktuální bezpečnostní situaci.
* Datových toků v síti – cílem je sběr dat o komunikaci komponent, aplikací a služeb pro analýzu normálního a abnormálního chování komponent, aplikací a služeb.
* Auditní záznamy – cílem je monitorování, zpracování a vyhodnocování přístupů k jednotlivým systémům včetně dodržování politiky hesel, změny v oprávnění uživatelů či zamykaní uživatelských účtů.
* Pravidel na firewallu – cílem je identifikace bezpečnostní politiky komunikačních pravidel komponent, aplikací a služeb v informačních systémech klienta a jejich harmonizace pro naplnění ochrany zákonem klasifikovaných informací klienta.
* Bezpečnostních politik – cílem je implementace bezpečnostních politik do dohledových nástrojů, která umožní jejich skutečnou aplikaci do kybernetického prostoru a následný monitoring.
* Specifických potřeby organizace – cílem je získat odborné konzultační služby, při kterých má organizace možnost využít know-how a best-practice specialistů dohledového centra dodavatele.
* Asset management – cílem je jasná definice rozsahu a pojmenování infrastruktury organizace.
* Zranitelnosti jednotlivých aktiv – cílem je pravidelně vyhodnocovat a řídit zranitelnosti v infrastruktuře organizace.

# Komunikace s Dodavatelem

Pro komunikaci Zadavatele s Dodavatelem musí být vytvořeno tiketovací procesní workflow k definici způsobů pro zabezpečenou komunikaci a výměnu dokumentů. Objednatel požaduje přidělení primárního specialisty Dodavatele, který bude s Objednatelem komunikovat identifikované nálezy a navrhovaná doporučení.

# Požadavky Zadavatele na kvalifikaci

Kvalifikovaným pro plnění veřejné zakázky je v souladu s ust. § 73 a násl. ZZVZ dodavatel, který prokáže splnění požadavků:

## Technická kvalifikace dle ust. § 79 ZZVZ

**Technickou kvalifikaci splňuje dodavatel, který předloží:**

* seznam významných zakázek realizovaných v posledních 3 letech před zahájením zadávacího řízení

**Způsob prokázání splnění technické kvalifikace (doklady):**

Předložení seznamu významných zakázek, v němž budou uvedeny alespoň následující údaje:

1. název objednatele,
2. předmět významné zakázky,
3. doba realizace významné zakázky (zahájení – měsíc/rok, dokončení – měsíc/rok),
4. finanční objem významné zakázky, je-li dále požadován,
5. kontaktní osoba objednatele, u které bude možné realizaci významné zakázky ověřit, vč. kontaktního e-mailu a telefonu

Dodavatel splňuje tuto technickou kvalifikaci, pokud za poslední 3 roky před zahájením zadávacího řízení poskytoval alespoň 3 (tři) významné dodávky/služby, které splňují následující čtyři požadavky:

1. každá významná dodávka/služba musela být poskytována v oblasti provozu služby Security Operations Centra (Bezpečnostního dohledového centra)
2. alespoň jedna významná dodávka/služba musela být ve finančním objemu minimálně 500 000 Kč bez DPH za jeden rok plnění
3. nejméně dvě významné dodávky/služby musely být ve finančním objemu minimálně 300 000 Kč bez DPH za jeden rok plnění
4. alespoň jedna významná dodávka/služba byla poskytnuta subjektu, který spravuje nebo provozuje alespoň jeden systém kritické informační infrastruktury nebo informační systém základní služby dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

Finančním objemem významných dodávek či služeb se rozumí cena bez DPH zaplacená za odvedené a objednatelem akceptované služby či dodávky.

**Dodavatel předloží doklady o odborné kvalifikaci pro následující osoby:**

K prokázání technické kvalifikace ve smyslu ustanovení § 79 odst. 2 písm. c) a d) zákona zadavatel požaduje po dodavateli **předložení seznamu techniků (realizačního týmu dodavatele)**, kteří se budou podílet na plnění veřejné zakázky. Požadované role nelze sdílet.

Zadavatel požaduje, aby se realizační tým dodavatele sestával nejméně z **7 (sedmi) odborníků**, kteří splňují níže uvedené požadavky:

* **Manažer SOC** (1 osoba) s níže uvedenými požadavky na jeho kvalifikaci:
* je držitelem platné certifikace z oblasti managementu kybernetické bezpečnosti (certifikace akreditovaná dle ISO/IEC 17024 nebo ISO 27001 anebo relevantní certifikace ISACA, nebo obdobný ekvivalent),
* má alespoň 5 let praxe za posledních 7 let před zahájením zadávacího řízení v oblasti kybernetické bezpečnosti
* (tato praxe musí vyplynout z profesního životopisu, kdy v každém příslušném roce dokládané praxe musela osoba vykázat alespoň jednu zkušenost v požadované oblasti; jedna zkušenost může být započítána i v rámci dvou (i více) let, a to za předpokladu, že v příslušném roce bylo plnění poskytováno alespoň po dobu 3 měsíců),
* **Forenzní analytik** (1 osoba) s níže uvedenými požadavky na jeho kvalifikaci:
* je držitelem platné technické certifikace související s technologií nabízených služeb v oblasti kybernetické bezpečnosti a certifikace CompTIA Sec+, CySa+, CEH nebo obdobné,
* má alespoň 5 let praxe za posledních 7 let před zahájením zadávacího řízení v oblasti kybernetické bezpečnosti (tato praxe musí vyplynout z profesního životopisu, kdy v každém příslušném
* roce dokládané praxe musela osoba vykázat alespoň jednu zkušenost v požadované oblasti; jedna zkušenost může být započítána i v rámci dvou (i více) let,
* má alespoň 1 zkušenost za posledních 5 let před zahájením zadávacího řízení se zpracováním informací o kybernetických bezpečnostních událostech a incidentech s využitím specializovaných metod analýzy dat a technik pro získávání důkazů souvisejících s případnou trestní činností
* **Analytik kybernetické bezpečnosti** (2 osoby) s níže uvedenými požadavky na jeho kvalifikaci:
* minimálně úplné dokončené středoškolské vzdělání,
* minimálně 2 roky praxe v oboru bezpečnostních technologií,
* zkušenost s provozováním SOC (dohledového centra) zahrnujícího alespoň sběr logů z více než 100 zařízení a vyhodnocováním logů s cílem identifikovat potenciální bezpečnostní incidenty,
* zkušenost s analytickými nástroji (uvedení konkrétních zkušeností).
* **Operátor SOC** (3 osoby) s níže uvedenými požadavky na jeho kvalifikaci:
  + minimálně úplné dokončené středoškolské vzdělání technického směru,
  + minimálně 1 rok praxe na pozici Operátor SOC.

Jako potvrzení splnění výše uvedených požadavků na realizační tým, bude zadavatel akceptovat předložení:

* seznamu pracovníků formou čestného prohlášení a s uvedením funkce v realizačním týmu u každého člena,
* profesních životopisů všech nominovaných členů,
* kopií dokladů o vzdělání pro všechny členy realizačního týmu,
* kopii osvědčení nebo certifikátů u rolí, kde jsou požadovány.

Ve strukturovaném profesním životopise bude uvedeno:

1. jméno, příjmení a titul,
2. dosažené vzdělání,
3. osvědčení či certifikáty (pokud je požadováno),
4. podrobný popis činnosti člena týmu na plnění veřejné zakázky;
5. údaj o zaměstnavateli, popř. IČO pracovníka
6. zkušenosti / praxe v minimálním rozsahu dle požadavků specifikovaných u každé role výše, tzn. přehled profesní praxe vztahující se k předmětu plnění veřejné zakázky, včetně délky praxe k datu podání žádosti. Je-li u pracovníka požadována účast na projektu, požaduje zadavatel, aby účastník zadávacího řízení v rámci profesního životopisu uvedl název objednatele, název zakázky či projektu a stručný popis zakázky či projektu včetně jeho délky,
7. jazykové schopnosti,
8. čestné prohlášení o úplnosti a pravosti údajů uvedených v příslušném profesním životopisu,
9. datum vypracování a vlastnoruční podpis člena realizačního týmu.

Účastník může uvést více pracovníků pro dané role, než zadavatel požaduje. V případě, že účastník navrhne ve své nabídce vyšší než minimální zadavatelem požadovaný počet osob na konkrétní pozici realizačního týmu, musí všechny takto dodavatelem navržené osoby na konkrétní pozici realizačního týmu splňovat v plném rozsahu kvalifikaci požadovanou zadavatelem pro příslušnou pozici realizačního týmu.

Zadavatel dále požaduje, aby v případě prokázání části kvalifikace jinou osobou (poddodavatelem), odpovídalo zastoupení pracovníků poddodavatele v realizačním týmu rozsahu a odbornosti, v jakém jiná osoba prokázala kvalifikaci za dodavatele v souladu s § 83 zákona.

Zadavatel upozorňuje, že se dodavatel v rámci trvání smluvního vztahu zaváže zachovat složení týmu pracovníků v souladu s požadavky stanovenými v kvalifikační dokumentaci s tím, že **osoby, kterými bude prokazováno splnění technické kvalifikace, se budou skutečně podílet na realizaci předmětu veřejné zakázky**. Postup v případě nutné personální změny bude podléhat odsouhlasení Zadavatelem.

# Další požadavky a práva zadavatele

Účastník je povinen ve své nabídce specifikovat části veřejné zakázky v hodnotě nad 500.000 Kč bez DPH, které má v úmyslu zadat jednomu či více poddodavatelům a je povinen uvést identifikační údaje všech těchto poddodavatelů včetně části, kterou bude poddodavatel realizovat. Účastník tak učiní prohlášením, k němuž využije přílohu č. 4 této ZD.

Účastník nemá právo na úhradu nákladů spojených s účastí v tomto zadávacím řízení a nepřísluší mu náhrada za zpracování a podání nabídky.

Zadavatel si vyhrazuje právo zveřejnit všechny informace, poskytnuté uchazeči v nabídkách nebo dalších požadovaných dokumentech, pokud se na ně nevztahuje ochrana podle ustanovení obecně platných právních předpisů. Zadavatel si rovněž vyhrazuje právo zveřejnit dokumenty zadavatele, týkající se průběhu zadávacího řízení.

Účastník zadávacího řízení prokáže řádné pojištění odpovědnosti za škodu vzniklou jeho činností, a to nejméně na částku 10.000.000,- Kč. Tuto výši pojištění bude udržovat po celou dobu platnosti smluvního vztahu a na vyžádání ji doloží kdykoliv za trvání smluvního vztahu (porušení povinnosti bude důvodem k ukončení smlouvy). Tato povinnost bude též zahrnuta v návrhu smlouvy předložené účastníkem. Účastník prokáže tuto část technické kvalifikace kopií dokladu dokládajícího existenci pojištění (např. kopie pojistné smlouvy).

Účastník podáním své nabídky vyslovuje souhlas se zveřejněním všech náležitostí budoucího smluvního vztahu (celé znění smlouvy včetně všech změn a dodatků). Zadavatel si vyhrazuje právo zrušit zadávací řízení do okamžiku uzavření Smlouvy.

Zadavatel si vyhrazuje právo ověřit si informace poskytnuté účastníkem u třetích osob a účastník je povinen mu v tomto ohledu poskytnout veškerou potřebnou součinnost.

Zadavatel nepřipouští varianty nabídky.

Účastník podáním nabídky prohlašuje:

* že bez výhrad souhlasí se zadáním a podmínkami zadávacího řízení,
* že si před podáním nabídky vyjasnil veškerá nejasná ustanovení a případné technické a jiné náležitosti,
* že všechny údaje uvedené v nabídce jsou pravdivé, že nezamlčel žádné skutečnosti podstatné pro jeho způsobilost k realizaci veřejné zakázky,
* že je připraven spolehlivě a bez průtahů splnit podmínky zadání a že v případě získání veřejné zakázky vyhradí potřebný čas a prostředky na realizaci veřejné zakázky,
* že na jeho straně neexistují majetkové ani právní překážky pro realizaci veřejné zakázky, a že nedošlo k událostem, na základě kterých by bylo možné zpochybnit jeho odbornou a morální způsobilost pro realizaci veřejné zakázky.

V případě, že bude účastníkem podána neúplná nabídka, tj. nabídka, která neobsahuje všechny doklady a dokumenty požadované zadavatelem v ZD, může být tato nabídka vyřazena a účastník vyloučen z účasti v zadávacím řízení.

# Způsob zpracování a členění nabídky

## Zpracování nabídky

Nabídka účastníka:

1. bude zpracována v českém jazyce; u veškerých listin a jiných dokumentů, jež jsou součástí nabídky a jsou vyhotoveny v jiném než českém jazyce, je nutný jejich překlad do českého jazyka, s výjimkou dokladů v jazyce slovenském,
2. bude obsahovat krycí list nabídky s uvedením identifikačních údajů zadavatele a účastníka, s uvedením Celkové nabídkové ceny; krycí list nabídky bude podepsán osobou oprávněnou jednat jménem či za účastníka; vzor je uveden v příloze č. 2 této ZD,
3. bude obsahovat jednu kontaktní adresu pro elektronický písemný styk mezi účastníkem a zadavatelem; pokud podává nabídku více účastníků společně, uvedou v nabídce kromě kontaktní adresy dle předchozí věty též osobu, která bude zmocněna zastupovat tyto účastníky při styku se zadavatelem v průběhu zadávacího řízení,
4. nesmí obsahovat přepisy a opravy, které by mohly zadavatele uvést v omyl,
5. bude obsahovat potvrzení technické kvalifikace dle odst. 10.1, jimiž účastník prokazuje splnění kvalifikace, ve formátu přílohy č. 3 této ZD
6. bude obsahovat smlouvu o společnosti (je-li nabídka podána více účastníky společně) nebo písemný závazek poddodavatele obdobně jako dle § 83 odst. 1 písm. d) zákona (je-li některý z kvalifikačních předpokladů prokázán prostřednictvím poddodavatele).
7. bude obsahovat písemnou plnou moc v případě, že je účastník zastoupen osobou, která není oprávněná jednat jeho jménem,
8. platné osvědčení podnikatele dle této ZD,
9. bude obsahovat seznam poddodavatelů s hodnotou poddodávky větší než 500.000,- Kč bez DPH dle odst. 9 této ZD; vzor tohoto seznamu je přílohou č. 4 této ZD

# Lhůta, způsob a místo pro podání nabídek

## Lhůta pro podání nabídky

Lhůta pro podání nabídek končí dne **16.8.2023 v 13:00 hod**.

## Způsob a místo podání nabídek

Každý účastník může podat pouze 1 nabídku do veřejné zakázky.

Nabídku může účastník podat pouze v elektronické podobě prostřednictvím elektronického nástroje E-ZAK (elektronický nástroj)

* na adrese <https://zakazky.vakpce.cz/>
* Systémové číslo VZ: **P23V00000011.**

Zadavatel upozorňuje na případná technická omezení vyplývající z podávání nabídky formou elektronického nástroje a zejména na potřebu včasné registrace dodavatelů do elektronického nástroje a s tím související nezbytným ověřením identity účastníků.

Zadavatel dále upozorňuje na možnost omezení velikosti podávaných nabídek, která je limitována technickými možnostmi nástroje E-ZAK. Jednotlivé dokumenty předkládané k nabídce musí být zpracovány prostřednictvím akceptovatelných formátů souborů.

Zadavatel dále uvádí k podání nabídky v elektronické podobě:

* Pro podání nabídky bude použit certifikovaný elektronický nástroj E-ZAK, který je dostupný na <https://zakazky.vakpce.cz/>.
* Dodavatel musí být pro možnost podání nabídky v elektronické podobě registrován jako dodavatel v elektronickém nástroji. Návod na provedení registrace je dostupný na stránkách elektronického nástroje.
* Zadavatel nenese odpovědnost za technické podmínky na straně dodavatele. Zadavatel doporučuje dodavatelům zohlednit zejména rychlost jejich připojení k internetu při podávání nabídky tak, aby byla podána ve lhůtě pro podání nabídky.

Nabídka včetně veškerých dokumentů a příloh bude zpracována v českém jazyce. Pokud účastník jako součást nabídky bude předkládat dokumenty i v jiném než českém jazyce, musí s nimi přiložit jejich překlad do českého jazyka (to neplatí v případě dokumentů ve slovenském jazyce, dokladů o vzdělání v latinském jazyce). V případě pochybností o předloženém překladu je zadavatel oprávněn žádat předložení úředně ověřeného překladu dokladu do českého jazyka tlumočníkem zapsaným do seznamu znalců a tlumočníků. Účastník může k nabídce přiložit prospekty a obdobné materiály sloužící pro informaci zadavatele, které nejsou povinnými doklady přikládanými k nabídce, a to i v jiném než českém jazyce.

Zadavatel si vyhrazuje právo ověřit a prověřit údaje uvedené jednotlivými účastníky v nabídce. Zadavatel vyloučí účastníka ze zadávacího řízení v případě, že účastník uvede ve své nabídce nepravdivé údaje.

Součástí nabídky bude rovněž vyplněný Krycí list nabídky, ve kterém budou uvedeny identifikační údaje účastníka, kontaktní adresa pro písemný styk mezi účastníkem a zadavatelem

## Zadavatel doporučuje, aby účastníci zpracovali nabídku v následujícím členění

* krycí list nabídky
* návrh smlouvy  včetně obchodních podmínek,
* další dokumenty, jsou-li požadovány touto zadávací dokumentaci

## Místo, způsob a lhůta pro podání nabídek

Nabídky se podávají písemně, a to v elektronické podobě prostřednictvím elektronického nástroje.

# Vysvětlení zadávací dokumentace

Účastníci zadávacího řízení jsou oprávněni požadovat vysvětlení zadávací dokumentace. Žádost o vysvětlení zadávací dokumentace musí být doručena zadavateli nejpozději 4 pracovní dny před prohlídkou místa plnění.

S ohledem na předmět veřejné zakázky zadavatel vyčlení termín pro prohlídku místa plnění VZ, a to dne **9.8.2023 od 9 hod. do 15 hod.** Před prohlídkou místa plnění musí být uchazečem předáno Prohlášení o mlčenlivosti dle přílohy č. 5, podepsané osobou, která je oprávněná jednat jménem uchazeče.

Telefonické dotazy nebudou akceptovány.

Zadavatel může poskytnout vysvětlení zadávací dokumentace i bez předchozí žádosti.

# Otevírání nabídek

Otevírání elektronicky podaných nabídek se uskuteční dne **17.8.2023** v sídle zadavatele. Otevírání obálek je z důvodů elektronického podání nabídek neveřejné.

# Požadavky na zpracování nabídek a jejich posouzení a hodnocení

Zadavatel uvádí, že pro posouzení a hodnocení nabídek je zadavatelem stanoven níže uvedený postup:

1. Každý dodavatel může podat pouze 1 nabídku.
2. Každá nabídka doručená zadavateli bude posouzena, zda obsahuje veškeré doklady požadované zadavatelem a vyplývající z této zadávací dokumentaci, a zda dodavatel splňuje podmínky a požadavky stanovené zadavatelem v této zadávací dokumentaci. Zadavatel je oprávněn, nikoliv však povinen, požádat každého účastníka o doplnění příp. chybějících dokladů či požadovat po dodavatelích vysvětlení.
3. Účastník, který bude vyhodnocen jako vítězný, bude vyzván k podpisu smlouvy. Zadavatel si před uzavřením smluvního vztahu vyhrazuje právo jednat s vybraným účastníkem o úpravách jeho návrhu smlouvy, k čemuž dotčený účastník poskytuje svou součinnost.
4. Neposkytne-li vybraný účastník dostatečnou součinnost k podpisu smlouvy, a ta nebude z důvodů na jeho straně podepsána do 15 dnů od vyzvání k jejímu podpisu, může zadavatel vyzvat k podpisu smlouvy účastníky, který se v konečném hodnocení umístil na dalším místě v pořadí.
5. Zadavatel stanovuje podmínku, že nabídková cena uchazeče nesmí přesáhnout předpokládanou hodnotu, tj. částku 2 999 999Kč bez DPH. **Překročení této maximálně přípustné ceny je důvodem k vyřazení uchazeče.**

## Hodnocení nabídek

Hodnotícím kritériem je ekonomická výhodnost nabídky, která bude hodnocena podle jediného hodnotícího kritéria, a to nejnižší nabídkové ceny v Kč bez DPH.

Nejvýhodnější nabídkou je nabídka s nejnižší nabídkovou cenou.

Za vybraného dodavatele bude považován ten, který nabídne nejnižší nabídkovou cenu za předmět plnění veřejné zakázky za současného splnění podmínek této Zadávací dokumentace.

# Přílohy

**Příloha ZD číslo 1. – Technická specifikace**

**Příloha ZD číslo 2. – Vzor krycího listu nabídky**

**Příloha ZD číslo 3. – Vzor čestného prohlášení o splnění technické kvalifikace**

**Příloha ZD číslo 4. – Seznam poddodavatelů nad 500 tis. Kč**

**Příloha ZD číslo 5. – Prohlášení o mlčenlivosti**