VÝZVA K PODÁNÍ NABÍDKY

STAREZ – SPORT, a.s.

se sídlem Křídlovická 34, 603 00 Brno, IČO: 269 32 211

(dále jen „*zadavatel*“) tímto

v y z ý v á

k podání nabídky ve výběrovém řízení na veřejnou zakázku malého rozsahu na dodávky

Dodávka technologie FIREWALL

(dále jen veřejná zakázka)

zadávanou mimo režim zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen zákon)

I. Preambule

1. Veškeré úkony v rámci výběrového řízení se provádějí elektronicky prostřednictvím elektronického nástroje E-ZAK dostupného na https://zakazky.starezsport.cz/ (nestanoví-li zadavatel v zadávacích podmínkách nebo v průběhu výběrového řízení jinak). Zadavatel dodavatele upozorňuje, že **pro plné využití všech možností elektronického nástroje E-ZAK je třeba provést a dokončit tzv. registraci dodavatele**. Vyřízení registrace trvá maximálně 48 hodin (v pracovní dny) a není zpoplatněno.
2. Zadavatel dodavatelům doporučuje, aby kontaktní osobu zadavatele požádali o přiřazení k veřejné zakázce nebo aby průběžně sledovali adresu veřejné zakázky.
3. Zavedl-li zadavatel dodavatele do elektronického nástroje E-ZAK, uvede u něj jako kontaktní údaje takové, které získal jako veřejně přístupné, nebo jiné vhodné kontaktní údaje. Je povinností každého dodavatele, aby před dokončením registrace do elektronického nástroje E-ZAK své kontaktní údaje zkontroloval a případně upravil či doplnil jiné.
4. Veškeré písemnosti zasílané prostřednictvím elektronického nástroje E-ZAK se považují za řádně doručené dnem jejich doručení do uživatelského účtu adresáta písemnosti v elektronickém nástroji E-ZAK. Na doručení písemnosti nemá vliv, zda byla písemnost jejím adresátem přečtena, případně, zda elektronický nástroj E-ZAK adresátovi odeslal na kontaktní emailovou adresu upozornění o tom, že na jeho uživatelský účet v elektronickém nástroji E-ZAK byla doručena nová zpráva, či nikoli.
5. Podrobné informace o ovládání systému naleznete v uživatelské příručce dostupné na: https://zakazky.starezsport.cz/
6. Zadavatel má zájem, s ohledem na povahu a smysl této veřejné zakázky, dodržovat zásady sociálně odpovědného zadávání, environmentálně odpovědného zadávání a inovací ve smyslu zákona, přičemž dodavatel je povinen tyto zásady dodržovat. Sociálně odpovědné zadávání kromě důrazu na čistě ekonomické parametry zohledňuje také související dopady zejména v oblasti zaměstnanosti, sociálních a pracovních práv a životního prostředí. Zadavatel od dodavatele vyžaduje při plnění předmětu veřejné zakázky zajistit zejména legální zaměstnávání, férové pracovní podmínky a odpovídající úroveň bezpečnosti práce pro všechny osoby, které se na plnění veřejné zakázky budou podílet. Dodavatel je povinen zajistit tento požadavek zadavatele i u svých poddodavatelů.

II. Předmět veřejné zakázky

Předmětem výběrového řízení je dodávka síťových bezpečnostních technologií (Firewall), technologií pro logování bezpečnostních událostí, autentizaci uživatelů umožňující MFA (multi-factor authentication), správa a podpora v oblasti kybernetické bezpečnosti.

Základní technické požadavky požadovaného řešení

- Zadavatel požaduje platformu postavenou na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, porovnávání se signaturovou databází).
- Celá dodávka musí obsahovat všechny HW komponenty a licence na dobu alespoň **2 let**.
- Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.
- Zadavatel požaduje dodání zařízení ve formátu HW appliance o velikosti 1RU.
- Zadavatel požaduje veškeré příslušenství (montážní prvky) pro montáž do RACKu.
- Možnost rozšíření platformy o další prvek typu NGFW jehož cílem bude zajišťování sdílení telemetrických informací, vizualizace stavu sítě, zařízení a klientů, přičemž celé řešení musí být podporováno výrobcem.
- Možnost o rozšíření platformy pro sběr logů a grafického reportingu včetně oboustranné komunikace (tím se rozumí minimálně odeslání a zpětné načítání logů pro účel vizualizace), přičemž zde musí existovat garantovaná podpora funkcionality.
- Součástí nabídky musí být také řešení pro logování síťových a bezpečnostních událostí detekovaných firewally a řešení umožňující autentizaci doménových uživatelů rozšířenou o druhý faktor provozované odděleně formou fyzické nebo virtuální appliance v prostředí zákazníka.
- Řešení musí zahrnovat dodávku FW ve vysoké dostupnosti v režimu minimálně 1+1.
- Možnost přístupu na webový portál výrobce HW s možností zadávat servisní požadavky a stahovat aktualizace firmwaru a softwaru.

HW parametry

- Počet síťových rozhraní copper, RJ45 10/100/1000 - min 16x;
- Počet GE SFP – min 8x ;
- Počet 10 GE SFP – min 4x (včetně min. 2x SFP+ fiber transceiverů s dosahem min. 250m);
- Konzolový port pro management;
- Dedikovaný port RJ45 pro management;
- Dedikovaný port RJ45 pro HA konfiguraci;
- USB 3.0 port pro zálohu konfigurace, případně pro připojení USB 4G modemu;
- Redundantní napájecí zdroj.

Výkonnostní parametry

- Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 26000 Mbps, 26000 Mbps, 10000 Mbps;
- Latence firewallu (64 B UDP paket) - max 5 mikro sec;
- Počet naráz otevřených spojení – min 2,7 M;
- Počet nových spojení za sekundu - min. 260 000;
- Počet firewall pravidel až 10 000;

- Podpora virtualizace (min 10 virtuálních kontextů);
- Podpora funkce bezdrátový kontrolér - 128 AP;
- Podpora funkce integrovaný switch controller – podpora až 64 switchů.

Funkce

Síťování a vysoká dostupnost

- Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IPsec SAs mezi nódy v clusteru;
- Režim fungování L2 – transparentní režim, L3 – NAT/Router;
- Podpora VLAN;
- Podopora multicast, vytváření politiky pro multicast routování;
- Podpora 802.3ad link aggregation;
- Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading;
- Podpora centrální NATovací tabulky, stavová inspekce SCTP komunikace;
- Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP;
- Policy-based routing;
- Funkce SD WAN – možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky.

VPN

- **Funkce SSL VPN**
  - Podpora klientského i bezklientského (portálového) režimu;
  - Minimální počet současně navázaných SSL VPN tunelů: 450;
  - Minimální propustnost SSL VPN: 1900Mbps.
- **Funkce IPSEC VPN**
  - podpora site-to-site VPN;
  - podpora klientských VPN;
  - dostupnost VPN klienta pro koncové stanice (Windows, MacOS);
  - funkce klientských IPSec VPN nesmí být licencovaná na počet uživatel. V opačném případě Zadavatel požaduje dodání neomezené licence;
  - Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 1900;
  - Minimální počet klientských IPSEC VPN tunelů: 15000;
  - propustnost IPSec VPN min. 12,5 Gbps (měřeno při AES256-SHA256);
  - podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování;
  - podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování;
  - podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace;
- Podpora VXLAN;
- Podpora L2TP, PPTP, GRE;
- podpora dynamických routovacích protokolů OSPF, BGP ve VPN IPsec.

Bezpečnostní funkce

- **Funkce detekce aplikací na L7 (Application Control)**
  - Detekce známých aplikací na základě signatur;
  - Signaturové databáze automaticky aktualizované výrobcem;
  - Propustnost funkce Application Control (HTTP 64K) minimálně 12000 Mbps;
  - alespoň 4000 podporovaných aplikací pro populární cloudové

aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) Zadavatel požaduje pokročilé akce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login, atd. (relevantní k dané aplikaci);
    - možnost tvorby vlastních signatur;
    - detekované aplikace je možné: povolit, monitorovat, blokovat;
    - na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci;
    - funkce AppCtr se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně Zadavatel požaduje možnost využití v rámci tzv. NGFW pravidel popsaných výše.
- **Funkce detekce a potlačení narušení (IPS/IDS)**
    - signatury automaticky aktualizované výrobcem;
    - alespoň 11.000 rozpoznávaných hrozeb (signatur) definovaných výrobcem;
    - možnost tvorby vlastních signatur;
    - funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům;
    - propustnost funkce IPS včetně logování min. 4800Mbps (měřeno na komunikaci typu mix aplikací).
- **Funkce antivirové kontroly**
    - Ochrana před škodlivým kódem (malware, trojské koně, atp.), včetně ochrany před polymorfním kódem;
    - Signatury automaticky aktualizované výrobcem;
    - Zadavatel požaduje AV kontrolu rozšířenou o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky);
    - možnost rozšíření o inspekci tzv. sandbox technikou formou lokální HW appliance stejného výrobce;
    - deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 2900 Mbps;
    - funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům;
    - Podpora služby výrobce, která umožní detekovat malware, který byl objevený v době od poslední aktualizace AV signaturové databáze pomocí globální a rychle se aktualizující databáze hashů;
    - Funkce odstranění aktivního obsahu z dokumentů kancelářských aplikací – AV engine na firewallu/bezpečnostní emailové bráně v reálném čase odstraní aktivní obsah z dokumentu, Dokument zůstává v původním formátu, jsou z něj odstraněny všechny aktivní prvky. Upravený dokument jde k původnímu příjemci, originální dokument se odešle do Sandboxu.
- **Funkce kategorizace webových stránek**
    - založená na centrálně spravované databázi výrobce;
    - minimálně 50 filtračních kategorií;
    - možnost definice vlastních kategorií;
    - možnost definice vlastních seznamů zakázaných URL;
    - kategorizace musí zahrnovat I české a slovenské internetové stránky.
- **Funkce DNS filtru**
    - Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobné kategorie jako u předchozího bodu);
    - Možnost definovat vlastní tzv. blacklist domén;
    - Možnost přesměrovat komunikace se zakázanými doménami na vlastní portal/URL;
    - Možnost importu seznamu blokovaných domén do DNS filtru;

    - Detekce a blokování komunikace do botnet sítí.
- **Funkce ochrany před únikem citlivých informací (DLP)**
    - možností analýzy běžných typů dokumentů a protokolů;
    - možnost definice pravidel min. na základě regulárních výrazů, watermarkovacího nástroje a typu kontroly typu file checksum;
- Email filter – jednoduchá antispamová a antivirová inspekce elektronické pošty;
- Podpora SSL dekrypce/SSL inspekce s minimální propustností 3900Mbps;
- DoS Policy prevence proti základním útokům typu DoS;
- Firewall musí být vybaven bezpečnostním modulem pro ukládání citlivých informací založeným na bázi HW (TPM).

Firewall

- Možnost nastavovat firewall politiku na základě geografických údajů;
- Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem;
- Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud;
- Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru;
- Viditelnost do provozu na aplikační úrovni;
- Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo);
- Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu;
- Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření;
- Traffic Shaping, QoS s podporou prioritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii;
- Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu
- Podpora funkce reverzní proxy;
- Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů;
- **Explicit proxy**
    - podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP);
    - podpora transparentního ověřování uživatel proti MS AD protokolem Kerberos;
    - funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta;
    - Funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatel na terminálovém serveru.

Integrovaný kontrolér bezdrátových (Wifi) sítí

- Wifi controller integrovaný do NGFW platformy;
- Každá bezdrátová síť (SSID) bude reprezentována virtuálním síťovým rozhraním;
- podpora bezpečnostních profilů (AV, AppControl, Webfilter, DLP) přímo na wifi controlleru;

- podpora SSL dekrypce uživatelského provozu přímo na wifi controlleru;
- Podpora wifi přístupových bodů stejného výrobce s výrobcem FW řešení;
- Možnost volby z různých modelů (např. 802.11abgn, 802.11ac, 802.11ac wave2, indoor, outdoor);
- On-wire rogue AP detekce a mitigace;
- Podpora fast-roamingu (802.11 k,v,r);
- podpora více PSK u jednoho SSID;
- podpora IPSEC tunelu pro šifrování data plane (uživatelských dat);
- podpora WPA3 šifrování;
- podpora WiFi 6 standardu;
- podpora BSS coloring (WiFi 6);
- podpora diagnostických WiFi nástrojů, například pro analýzu spektra.

Virtualiazce

- Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů, atp.;
- Součástí dodávky musí být licence na min. 10 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech);
- Každý virtuální kontext je zároveň samostatným wifi kontrolerem;
- Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů).

Management

- FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici;
- Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě;
- Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury).

Logování

Systém musí být plně kompatibilní s dodávanými zařízeními, musí podporovat analýzu logů nad provozem. Dále musí být schopné poskytovat reporty nad logy a informovat správce systému o hrozbách, které byly v síti odhaleny.

Celá dodávka musí obsahovat všechny HW a SW komponenty a licence na dobu **2 let**. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.

Hlavní požadavky:

- Musí se jednat o virtuální appliance s podporou minimálně VMware, KVM a Hyper-V stejného výrobce jako současného NGFW;
- Minimální limit pro množství přijatých logů za jeden den: 10GB;
- Možnost kontroly logů vůči databázi kompromitovaných zdrojů (IoC) minimálně pro stejné množství zdrojů jako je minimální limit;
- Podpora minimálně 4 virtuálních interface;
- Možnost škálovatelného navýšení kapacity úložiště na základě licence;
- Možnost provozovat appliance pouze jako dočasné úložiště logů z důvodu šetření datového pásma;

- Mít možnost specifikovat typ logů, které budou na hlavní analyzační nástroj odeslány okamžitě.

Multitenantnost

- Možnost rozdělení zařízení na oddělené administrativní sekce (každý virtuální kontext firewallu může být v jiném administrativním kontextu centrálního logovacího zařízení);
- Každý administrativní celek musí mít možnost mít vlastního administrátora, který nebude mít přístup do jiných administrativních celků.

Logovací funkce

- Musí se jedna o centrální logovací prvek pro všechny firewally;
- Musí umět ukládat jakkoliv Syslog zprávy;
- Funkce zpětné kontroly logů o přístupu na web (až 7 dní) z důvodu „zero-day" malicious websites;
- Vizualizace provozu nad všemi firewally;
- Možnost dostat se z vizuálního zobrazení proklikem na konkrétní logy;
- Realtime a historický náhled do logů;
- Korelace logů;
- Samostatná sekce týkající se hrozeb v síti;
- Podpora prohlížení statistických údajů nad logy;
- Funkce zpětné kontroly logů až 7 dnů zpět a zjištění, jestli systém nebyl napaden při přístupu na škodlivou webovou stránku. Logy jsou kontrolovány oproti pravidelně aktualizované databázi podezřelých IP adres, domén nebo webových URL adres.

Reporting

- Podpora reportů nad logy ve formátu HTML/CSV/XML/PDF;
- Generování reportů v pravidelných intervalech;
- Předefinované vzory pro reporty na nejčastější použití;
- Možnost vytváření vlastních reportů na základě konkrétních SELECT dotazů do databáze;
- Možnost úpravy reportů do vlastního designu – vlastní loga, texty, úprava hlavičky.

Další funkce

- Event Management – upozorňování na důležité informace z logů – emailem a snmp trapy, syslog zprávou;
- Předvytvořený dashboard pro využití dohledovým centrem;
- Možnost rozšíření o funkce SOC – parsování, analýza a korelace logů. Následná automatizovaná odpověď na incidenty za účelem blokace dané hrozby na NGFW stejného výrobce, případně karanténa klienta. Automatizované odpovědi mohou být definovány administrátorem, případně je možno využít vzorové scénáře.
    - Možnost customizace rozhraní pro NOC/SOC;
    - Incident Management – management incidentů vytvořených ze vzniklých eventů v SOC rozhraní;
    - PlayBook Automatizace – automatizované odpovědi na incidenty dle vzorových scénářů;
- Outbreak služba – v případě rychle šířící se kybernetické hrozby vyhodnocené výrobcem systému může administrátor tohoto systému zobrazit varování a k tomu odpovídající event handlery a předdefinované reporty. Administrátor následně může prohledat pomocí daných reportů stávající logy na zařízení za účelem identifikace daného malwaru.

Možnosti správy a komunikace

- Podpora SNMPv2, SNMPv3;
- Podpora REST API;
- Správa přes webové rozhraní HTTPS;
- Administrátorské účty musí být možné konfigurovat lokálně nebo na vzdáleném serveru (LDAP, RADIUS, Tacacs+);
- Podpora statického routování;
- Možnost zašifrování spojení mezi zařízením, které odesílá logy a analyzačním nástrojem, který je předmětem této zadávací dokumentace.

Autentizace

Systém musí být kompatibilní s dodanými technologiemi a podporovat několik druhů autentizace uživatelů popsaných níže. Zároveň musí umožňovat zavedení second faktor authentication (2FA) a vše s podporou výrobce alespoň 2 roky.

Hlavní požadavky

- Autentizaci min. pro **100 uživatelů**;
- Podpora alespoň. 200 mobilních tokenů;
- Podpora virtualizace, pakliže se jedná o virtuální appliance min.: VMware ESXi/ ESX 6/ 7/ 8, Microsoft Hyper-V Server 2010, 2012 R2, and 2016, Microsoft Azure, AWS;
- Podpora vysoké dostupnosti v režimu: Active-Passive;
- Podpora Single Sign-On;
- Secure Multifactor/OTP autentizace;
- Podpora Radius, LDAP, AD, SAML SP/IdP, FIDO 2;

Požadavky na mobilní token

- Minimálně pro **10 uživatelů**;
- Mobilního klíč ve formě aplikace na mobilní telefon s podporou platforem: iOS, Android, Windows;
- OTP splňující alespoň normy: RFC 6238, RFC 4226;
- Podpora PUSH notifikací s podporou zobrazení přihlašovacích informací;
- Ochrana aplikace pomoci PIN, Fingerprint a Facial recognition;
- Ochrana proti brute-force útoku.

Předmět veřejné zakázky je podrobně specifikován v příloze B této výzvy (závazné obchodní podmínky), které obsahují požadavky zadavatele na plnění veřejné zakázky. Tyto požadavky je dodavatel povinen respektovat.

III. Předpokládaná doba plnění

Dodání do **jednoho měsíce** od nabytí účinnosti smlouvy uzavřené na základě tohoto výběrového řízení.

IV. Místo plnění a prohlídka místa plnění

Místem plnění je STAREZ – SPORT, a.s., Ponávka 808/3a, 602 00 Brno-město.

V. Lhůta pro podání nabídky

Lhůta pro podání nabídek: **do 14. 12. 2023 do 12.00 hodin.**

VI. Místo pro podání nabídky

Nabídky se podávají prostřednictvím elektronického nástroje na adrese veřejné zakázky.

VII. Požadavky zadavatele na kvalifikaci

Dodavatelé jsou povinni prokázat kvalifikaci požadovanou zadavatelem. Požadavky na kvalifikaci jsou zadavatelem stanoveny ve formuláři nabídky. Dodavatel, který nesplní kvalifikaci požadovaným způsobem a v požadovaném rozsahu, může být zadavatelem z účasti ve výběrovém řízení vyloučen.

VIII. Závaznost obecných zadávacích podmínek a vysvětlení, změna nebo doplnění zadávací dokumentace

a) Závaznost požadavků zadavatele

Informace a údaje uvedené v této výzvě vymezují závazné požadavky zadavatele na plnění veřejné zakázky. Dodavatel, který nesplní stanovené požadavky zadavatele, může být zadavatelem z účasti ve výběrovém řízení vyloučen.

b) Vysvětlení, změna nebo doplnění zadávací dokumentace

Žádost o vysvětlení může účastník zasílat zadavateli elektronicky prostřednictvím elektronického nástroje. Zadavatel je oprávněn uveřejnit na profilu zadavatele vysvětlení zadávací dokumentace i z vlastního podnětu. Takto může rovněž uveřejnit změnu nebo doplnění zadávací dokumentace. Pokud to povaha doplnění nebo změny zadávací dokumentace vyžaduje, zadavatel současně přiměřeně prodlouží lhůtu pro podání nabídek.

IX. Obsah nabídky

Zadavatel přílohou zadávací dokumentace předkládá dodavatelům vzorový **formulář nabídky** obsahující požadavky zadavatele, kterými je podmiňována účast dodavatelů ve výběrovém řízení.

Splnění veškerých požadavků zadavatele, tj. požadavků na předmět veřejné zakázky, na kvalifikaci nebo na předložení údajů rozhodných pro hodnocení, prokáží dodavatelé předložením formuláře nabídky včetně příslušných příloh nebo jiných rovnocenných dokladů.

Zadavatel stanovuje, že nabídka uchazeče musí obsahovat tyto dokumenty:

a) formulář nabídky

Návrh smlouvy ani ostatní dokumenty nemusí být do nabídky přikládány.

V případě rozporu mezi celkovou nabídkovou cenou zapsanou ve formuláři nabídky a mezi celkovou nabídkovou cenou uvedenou jinde v textu nabídky nebo jejích přílohách, budou pro účely hodnocení nabídek a realizaci plnění použity údaje uvedené ve formuláři nabídky.

X. Způsob výběru nejvhodnější nabídky (hodnocení nabídek)

Hodnocení nabídek bude provedeno podle základního hodnotícího kritéria ekonomická výhodnost nabídky, a to na základě nejnižší nabídkové ceny. Hodnotící komise podle výše nabídkové ceny určí pořadí nabídek. Jako nejvhodnější nabídka bude hodnocena nabídka s nejnižší nabídkovou cenou v Kč bez DPH uvedenou ve formuláři nabídky.

XI. Kontaktní osoba zadavatele

Kontaktní osobou zadavatele ve věcech souvisejících s tímto výběrovým řízením je Mgr. David Zuska, tel. +420 737 566 827, email: zuska@starezsport.cz nebo Mgr. Rostislav Gnida, tel. +420 734 690 922, email: gnida@starezsport.cz.

XII. Závěrečná ustanovení

Účastník výběrového řízení nemá nárok na úhradu nákladů souvisejících s účastí ve výběrovém řízení (např. nákladů na zpracování nabídky).

Zadavatel je oprávněn ověřovat údaje uvedené účastníkem výběrového řízení v nabídce. V případě, že zadavatel zjistí, že informace uvedené v nabídce účastníka nejsou pravdivé, je zadavatel oprávněn takového účastníka vyloučit z další účasti ve výběrovém řízení.

Zadavatel je oprávněn požadovat po účastníkovi objasnění nebo doplnění nabídky. V případě, že účastník na výzvu zadavatele nabídku neobjasní nebo nedoplní, je zadavatel oprávněn vyloučit účastníka z další účasti ve výběrovém řízení.

Zadavatel si vyhrazuje právo výběrové řízení zrušit bez udání důvodu.

Zadavatel jako správce osobních údajů informuje subjekty údajů, od nichž obdrží nabídku, že osobní údaje zpracovává výhradně z důvodu a za účelem splnění právních povinností stanovených zákonem č. 134/2016 Sb., o zadávání veřejných zakázek.

Přílohy

A. Formulář nabídky

B. Obchodní podmínky

V Brně dne 4. 12. 2023

Mgr. Martin Mikš, generální ředitel

STAREZ – SPORT, a.s.