Příloha B výzvy

OBCHODNÍ PODMÍNKY

veřejné zakázky malého rozsahu

Zajištění síťových bezpečnostních technologií (FIREWALL)

STAREZ – SPORT, a.s.

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

PŘEDLOHA SMLOUVY O DÍLO

Veškeré technické, obchodní a jiné smluvní podmínky, které jsou zadavatelem zpracovány ve formě předlohy smlouvy, **musí být vybraným dodavatelem plně respektovány**. Zadavatel **nevyžaduje, aby byl návrh smlouvy předložen** v nabídce.

Smlouva o zajištění služeb v oblasti síťových bezpečnostních technologií (FIREWALL)

kterou podle ustanovení § 1746 odst. 2 a násl. zákona č. 89/2012 Sb., občanský zákoník (dále jen „***občanský zákoník***"), s přihlédnutím k § 2358 a násl. občanského zákoníku a zákonu č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „***autorský zákon***"), uzavřely níže uvedeného dne, měsíce a roku tyto smluvní strany:

STAREZ – SPORT, a.s.

se sídlem:	Křídlovická 911/34, 603 00 Brno
IČO:	26932211
DIČ:	CZ26932211
plátce DPH	
společnost zapsaná	v OR u Krajského soudu v Brně pod sp. zn. B 4174
bankovní spojení:	Komerční banka a.s., číslo účtu: 35-1393300227/0100, ověřený bankovní účet
společnost zastoupená:	Mgr. Martinem Mikšem, generálním ředitelem
kontaktní osoba:	……..
	Telefon:+420 …….
	E-mail: ……

dále jen „***objednatel***"

a

…….

se sídlem:	……..
IČO:	……..
DIČ:	……..
plátce DPH	
společnost zapsaná	……..
bankovní spojení:	……..
zastoupená	……..
kontaktní osoba:	……..
	Telefon: ……..
	E-mail: ……..

dále jen „***zhotovitel***"

I. Účel smlouvy

I.1. Účelem této smlouvy je uspokojení potřeby objednatele spočívající v zajištění služeb v oblasti síťových bezpečnostních technologií (FIREWALL).

II. Předmět smlouvy

II.1. Předmětem smlouvy je zajištění služeb v oblasti síťových bezpečnostních technologií (FIREWALL), technologií pro logování bezpečnostních událostí, autentizaci uživatelů umožňující MFA (multi-factor authentication), správy a podpory v oblasti kybernetické bezpečnosti.

II.2. Nedílnou součástí služeb je také audit klíčové síťové infrastruktury, který bude sloužit k identifikaci případných slabých míst a rizik a navrhne případné zlepšení, včetně jejich prověření etickým hackingem podle vymezených technických podmínek (specifikace).

II.3. **Základní technické požadavky**

- 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 cele 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.

Základní požadavky k poptávaným službám

Servisní podpora

Po dobu **1 roku** v režimu min. 8x5 s min. následujícími parametry v ceně:

- SLA 4h response;
- Aktualizace firmwaru Dodavatelem zařízení minimálně každé 3 měsíce a podpora proaktivní kontroly zařízení 1x krát měsíčně;
- Dále je požadován monitoring zařízení v režimu 24x7 monitorovacím řešením Dodavatele;
- ServiceDesk s možnosti kontaktovat Dodavatele minimálně následujícími způsoby: WEB, email, telefon;
- Předplacené hodiny konzultace v rozsahu min. 1 člověkoden/měsíčně;

Nasazení řešení

Součástí základního dodání musí být dodání HW a SW vybavení, vybalení, umístění, likvidace obalu, zapojení, připojení k napájení a LAN, konfigurace základních parametrů, nasazení a nastavení logování, testování fyzické redundance a dokumentace.

Dále zadavatel požaduje možnost konfigurace funkcí firewallu podle pokynů a potřeb prostředí Zadavatele nad rámec základního dodání výše o minimální velikosti **4** člověkodní [MDs].

Požadavky na audit sítě

Dodavatel s příslušnými znalostmi a zkušenostmi v oblasti bezpečnosti sítí a auditu síťové infrastruktury splňující minimálně požadavky zadavatele uvedené ve formuláři nabídky

Audit bude zahrnovat alespoň následující oblasti:

- síťový design a architektura;
- ochrana perimetru;
- segmentace sítě;
- nastavení firewallu;
- nastavení síťových zařízení;
- síťovou autentizaci;
- nástroje monitorování sítě a bezpečný internetový přístup;
- test exploitace vybrané zranitelnosti dle požadavku Zadavatele penetračním testerem.

Provedení auditu v každé z uvedených oblastí na základě předem získané dokumentace a schůzky v prostorách dodavatele, lokalita **Brno**.

Podrobná dokumentace zjištěných slabých míst, rizik a doporučených zlepšení v každé z uvedených oblastí.

Zpráva závěrečného hodnocení, která shrne výsledky auditu a doporučené nápravy.

III. Povinnosti zhotovitele

III.1. Zhotovitel se zavazuje řádně, včas, na svůj náklad a nebezpečí vykonávat pro objednatele celý předmět plnění dle této smlouvy v souladu s technickou specifikací.

III.2. Při výkonu své činnosti dle této smlouvy se zhotovitel zavazuje postupovat samostatně a s odbornou péčí tak, aby byl zcela a včas naplněn účel této smlouvy.

III.3. Při realizaci předmětu smlouvy je objednatel oprávněn uplatnit písemně požadavky a připomínky a dát zhotoviteli pokyny. Zhotovitel tyto připomínky a požadavky objednatele ve svém dalším postupu zapracuje a pokyny objednatele se při plnění svých povinností řídí. Zhotovitel je povinen upozornit objednatele bez zbytečného odkladu na nevhodnou povahu požadavků, připomínek a pokynů daných mu objednatelem při plnění předmětu smlouvy, jestliže zhotovitel mohl a měl tuto nevhodnost zjistit při vynaložení odborné péče.

III.4. Zhotovitel se zavazuje pro objednatele provádět plnění dle této smlouvy osobně nebo prostřednictvím jím pověřených zaměstnanců nebo prostřednictvím poddodavatele.

III.5. Zhotovitel je povinen uchovávat adresy URL, uživatelská jména a hesla objednatele v tajnosti. Zhotovitel nesmí za žádných okolností sdílet tyto informace s třetí

stranou, a to ani po skončení spolupráce s objednatelem. Zhotovitel odpovídá za jakoukoli újmu či škodu, která by vznikla v důsledku porušení této jeho povinnosti.

IV. Povinnosti objednatele

IV.1. Objednatel se zavazuje řádně poskytnuté plnění dle této smlouvy od zhotovitele převzít a zaplatit cenu ve výši a za podmínek sjednaných touto smlouvou.

IV.2. Objednatel se zavazuje poskytnout zhotoviteli k výkonu jeho činnosti dle této smlouvy nezbytnou součinnost a zajistit spolupráci odpovědných osob objednatele, které jsou z titulu své funkce schopny poskytnout zhotoviteli potřebné podklady a informace pro řádné a včasné splnění závazků zhotovitele vyplývající z této smlouvy.

V. Doba plnění

V.1. Smlouva je uzavřena na období dvou let od nabytí její účinnosti.

VI. Místo plnění

VI.1. Služba je poskytována vzdáleným přístupem nebo na místě u objednatele podle povahy poskytované služby.

VII. Cena

VII.1. Smluvní strany se dohodly, že cena díla činí **.....,- Kč bez DPH.**

VII.2. Ke sjednané ceně bez DPH bude připočtena DPH dle sazby stanovené dle platných a účinných obecně závazných právních předpisů.

VII.3. Výše ceny za poskytnutí plnění zhotovitelem dle této smlouvy je nejvýše přípustná a tuto je možno překročit pouze v případě zvýšení sazby DPH v rozsahu zákonné změny výše sazby DPH.

VII.4. Cena za poskytnutí plnění zahrnuje všechny náklady zhotovitele na jeho řádnou realizaci, vč. nákladů na dopravu, správních poplatků atd.

VII.5. V případě zvýšení sazby DPH se o zvýšenou část DPH zvyšují ceny nebo úplaty za poskytnutí jednotlivých plnění zhotovitelem dle této smlouvy, a to v poměru odpovídajícím zvýšení sazby DPH. V případě snížení sazby DPH se o sníženou část DPH snižují ceny nebo úplaty za poskytnutí jednotlivých plnění zhotovitelem dle této smlouvy, a to v poměru odpovídajícím snížení sazby DPH.

VIII. Platební podmínky

VIII.1. Podkladem pro platbu objednatele je daňový doklad – faktura.

VIII.2. Splatnost faktury se sjednává lhůtou 30 dnů od jejího doručení objednateli.

VIII.3. Daňový doklad – faktura musí obsahovat veškeré náležitosti daňového dokladu stanovené v zákoně č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a § 435 občanského zákoníku.

VIII.4. Objednatel je oprávněn před uplynutím lhůty splatnosti vrátit zhotoviteli fakturu, která neobsahuje požadované náležitosti, nebo obsahuje nesprávné údaje. Oprávněným vrácením faktury přestává běžet lhůta její splatnosti. Zhotovitel

vystaví novou fakturu se správnými údaji a dnem jejího doručení objednateli začíná běžet nová lhůta splatnosti.

VIII.5. Objednatel neposkytuje zálohy.

VIII.6. Platba vč. DPH dle této smlouvy bude hrazena v korunách českých, a to bezhotovostním převodem na účet zhotovitele. Cena za poskytnutí plnění se považuje za uhrazenou okamžikem odepsání fakturované ceny z bankovního účtu objednatele ve prospěch účtu zhotovitele. Bankovní účet zhotovitele musí být zveřejněn správcem daně způsobem umožňujícím dálkový přístup. V případě, že účet tímto způsobem zveřejněn nebude, je objednatel oprávněn uhradit zhotoviteli cenu na úrovni bez DPH. DPH Objednatel poukáže správci daně. Stane-li se zhotovitel nespolehlivým plátcem ve smyslu § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, je povinen neprodleně o tomto písemně informovat objednatele.

IX. Odpovědnost za vady a odpovědnost za škodu

IX.1. Dílo má vady, jestliže zpracování neodpovídá smlouvě, požadavkům, připomínkám nebo pokynům uplatněným objednatelem v průběhu poskytování plnění zhotovitelem dle této smlouvy nebo jestliže je plnění neúplné tak, že z důvodu jeho neúplnosti není možné pokračovat ke splnění účelu této smlouvy.

IX.2. Zjistí-li objednatel, že zhotovitel při výkonu činností dle této smlouvy postupuje v rozporu se svými povinnostmi, je oprávněn požadovat, aby zhotovitel bezodkladně odstranil vady vzniklé vadným poskytováním plnění dle této smlouvy a aby při výkonu činností dle této smlouvy postupoval řádně a v souladu s touto smlouvou. Neučiní-li tak zhotovitel ani v přiměřené lhůtě poskytnuté mu objednatelem, je možné tento stav považovat za podstatné porušení smlouvy ze strany zhotovitele.

IX.3. Vady je objednatel oprávněn uplatnit u zhotovitele písemně, bez zbytečného odkladu poté, co vady zjistí. V reklamaci je objednatel povinen vady popsat, popřípadě uvést, jak se projevují.

IX.4. Zhotovitel je povinen vady uplatněné objednatelem odstranit bezodkladně, nebude-li sjednána lhůta odlišná. Zhotovitel je povinen odstranit vady včas i v případě, že bezplatné odstranění vad neuznává. V těchto sporných případech nese zhotovitel náklady na odstranění vad až do doby, kdy dojde k dohodě smluvních stran o úhradě nákladů nebo do doby rozhodnutí o úhradě nákladů k odstranění vad právní cestou.

IX.5. O odstranění reklamované vady sepíše objednatel protokol, ve kterém potvrdí odstranění reklamované vady, nebo sdělí důvody odmítnutí reklamované vady.

IX.6. Jestliže nedojde k nápravě bez zbytečného odkladu po upozornění na zjištěné vady, nebo v dohodnuté lhůtě, nebo jestliže náprava již není možná, má objednatel právo na přiměřenou slevu z ceny díla.

X. Sankce a úroky z prodlení

X.1. Bude-li objednatel v prodlení s úhradou oprávněně ve vztahu k jeho osobě vystavené faktury proti sjednanému termínu, je zhotovitel oprávněn účtovat objednateli úrok z prodlení ve výši 0,1 % z částky v Kč bez DPH, s jejíž úhradou je

objednatel v prodlení, a to za každý i započatý den prodlení, až do doby zaplacení dlužné částky.

X.2. Úroky z prodlení jsou splatné na účet zhotovitele do 30 dnů od doručení písemné výzvy zhotovitele k zaplacení úroků, která obsahuje zhotovitelem vyúčtované úroky včetně způsobu jejich výpočtu.

X.3. Bude-li zhotovitel v prodlení s plněním díla, má objednatel vůči zhotoviteli právo na zaplacení smluvní pokuty ve výši ve výši 500,- Kč bez DPH za každý započatý den prodlení, a to za každý započatý den prodlení, a zhotovitel se zavazuje takto požadovanou smluvní pokutu zaplatit.

X.4. Nesplní-li zhotovitel včas svůj závazek dle této smlouvy řádně odstranit objednatelem uplatněné vady, je objednatel oprávněn požadovat na zhotoviteli zaplacení smluvní pokuty ve výši 500,- Kč bez DPH za každý započatý den prodlení, a to za každý započatý den prodlení anebo až do doby, kdy objednatel pověří odstraněním reklamovaných vad jinou odborně způsobilou právnickou nebo fyzickou osobu, a zhotovitel je povinen takto požadovanou smluvní pokutu objednateli zaplatit.

X.5. Vedle smluvních pokut dle tohoto článku smlouvy má objednatel právo na náhradu škody vzniklé mu v příčinné souvislosti s jednáním, nejednáním či opomenutím zhotovitele, s nímž je spojena smluvní pokuta dle této smlouvy.

X.6. Smluvní pokuty jsou splatné na účet objednatele do 21 dnů od doručení písemné výzvy objednatele k zaplacení příslušné smluvní pokuty zhotoviteli.

XI. Ukončení smluvního vztahu

XI.1. Tuto smlouvu lze ukončit buď dohodou smluvních stran, výpovědí nebo odstoupením některé smluvní strany.

XI.2. Ukončení smluvního vztahu musí být učiněno písemně, jinak je neplatné. Výpovědní doba činí tři měsíce a začíná běžet v měsíci následujícím po doručení výpovědi.

XI.3. Objednatel má právo od smlouvy odstoupit v případě podstatného porušení smlouvy zhotovitelem, pokud je konkrétní porušení povinnosti zhotovitelem jako podstatné sjednané v této smlouvě nebo v případě splnění zákonných podmínek podstatného porušení smlouvy ve smyslu ust. § 2002 odst. 1 občanského zákoníku.

XI.4. Smluvní strany se dohodly, že za podstatné porušení smlouvy ze strany zhotovitele považují zejména:

a) prodlení zhotovitele s poskytnutím plnění dle této smlouvy oproti době plnění dle čl. V této smlouvy delší než 30 dnů,

b) ostatní případy podstatného porušení smlouvy ze strany zhotovitele výslovně v této smlouvě označené jako podstatného porušení smlouvy.

XI.5. Za podstatné porušení smluvní povinnosti objednatele se považuje prodlení objednatele s úhradou ceny za plnění o více než 30 dnů, pokud objednatel nezjedná nápravu ani do 10 pracovních dnů od doručení písemného oznámení zhotovitele o takovém prodlení se žádostí o jeho nápravu.

XI.6. Odstoupení od smlouvy musí mít písemnou formu a je účinné dnem doručení druhé smluvní straně. V odstoupení musí být dále uveden důvod, pro který strana od smlouvy odstupuje, včetně popisu skutečností, ve kterých je tento důvod spatřován.

XI.7. V případě ukončení smluvního vztahu dohodou, výpovědí nebo odstoupením jsou povinnosti obou stran následující:

a) Zhotovitel dokončí rozpracovanou část plnění, pokud objednatel neurčí jinak;

b) Zhotovitel provede soupis všech jím vykonaných činností a úkonů ke splnění jeho závazků dle této smlouvy do doby ukončení smlouvy a dále provede soupis všech dokumentů získaných při zařizování záležitostí dle této smlouvy do doby jejího ukončení (dále jen „***soupis***");

c) Zhotovitel vyzve objednatele k protokolárnímu převzetí všech plnění dle soupisu na základě protokolu podepsaného smluvními stranami;

d) Objednatel není povinen soupis převzít, pokud obsahuje nesprávné údaje,

e) Zhotovitel provede vyúčtování plnění dle protokolu a vystaví závěrečnou fakturu.

XI.8. Na zhotovitelem poskytnuté plnění se i po ukončení této smlouvy vztahují ujednání o odpovědnosti za vady, slevy, smluvní pokuty a náhrady škody za vadné plnění.

XII. Zvláštní ujednání a ochrana osobních údajů

XII.1. Zhotovitel není oprávněn bez souhlasu objednatele postoupit závazky plynoucí z této smlouvy třetí osobě.

XII.2. Zhotovitel se zavazuje k veškeré nezbytné součinnosti pro výkon finanční kontroly ve smyslu zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, a ze zákona č. 255/2012 Sb., o kontrole (kontrolní řád), a to v souvislosti s plněním předmětu této smlouvy.

XII.3. Smluvní strany tímto společně prohlašují, že jsou si vědomy vzájemných práv a povinností dle zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů (dále také jen „ZZOÚ") a Nařízení Evropského parlamentu a Rady (EU) č. 2016/679, obecné nařízení o ochraně osobních údajů (dále také jen „GDPR"), zejména pak povinností stíhající jak správce osobních údajů, tak i zpracovatele osobních údajů, zejména povinnost zpracovávat osobní údaje korektně a zákonným a transparentním způsobem. Smluvní strany se zavazují osobní údaje zpracovávat takovým způsobem, který zaručí náležitou bezpečnost a důvěrnost těchto údajů, mimo jiné za účelem zabránění neoprávněnému přístupu k osobním údajům a k zařízení používanému k jejich zpracování nebo jejich neoprávněnému použití.

XII.4. V případě, že jedna ze smluvních stran zjistí, že došlo či je důvodné podezření, že by mohlo dojít k porušení z povinnosti či povinností plynoucí z GDPR nebo ZZOÚ je tato strana bez zbytečného odkladu povinna vyrozumět o této skutečnosti druhou smluvní stranu.

XII.5. Nad rámec povinností stanovených ZZOÚ a GDPR se smluvní strany navzájem zavazují postupovat při nakládání s osobními údaji ohleduplně a eticky tak, aby nevznikla ani jedné ze smluvních stran či třetí osobě v souvislosti se zpracováním osobních údajů újma.

XIII. Závěrečná ujednání

XIII.1. Práva a povinnosti smluvních stran výslovně touto smlouvou neupravené se řídí příslušnými ustanoveními občanského zákoníku a prováděcími předpisy.

XIII.2. Smluvní strany se dohodly, že zhotovitel výslovně souhlasí se zveřejněním smluvních podmínek obsažených v této smlouvě v rozsahu a za podmínek vyplývajících z obecně závazných právních předpisů.

XIII.3. Smlouva je vyhotovena ve dvou vyhotoveních, z nichž každé má platnost originálu. Jedno vyhotovení smlouvy obdrží objednatel, jedno vyhotovení obdrží zhotovitel.

XIII.4. Smlouvu je možno měnit pouze na základě dohody smluvních stran formou písemných číslovaných dodatků podepsaných oběma smluvními stranami.

XIII.5. Veškeré případné spory ze smlouvy budou v prvé řadě řešeny smírem. Pokud smíru nebude dosaženo během 30 dnů, všechny spory ze smlouvy a v souvislosti s ní budou řešeny věcně a místně příslušným soudem v České republice.

XIII.6. Žádné ustanovení smlouvy nesmí být vykládáno tak, aby omezovalo oprávnění objednatele uvedená v zadávací dokumentaci veřejné zakázky.

XIII.7. Smluvní strany se podpisem smlouvy dohodly, že vylučují aplikaci ustanovení § 557 a § 1805 občanského zákoníku.

XIII.8. Smluvní strany si nepřejí, aby nad rámec výslovných ustanovení smlouvy byla jakákoliv práva a povinnosti dovozovány z dosavadní či budoucí praxe zavedené mezi smluvními stranami či zvyklostí zachovávaných obecně či v odvětví týkajícím se předmětu plnění smlouvy, ledaže je ve smlouvě výslovně sjednáno jinak.

XIII.9. Pro vyloučení pochybností zhotovitel výslovně potvrzuje, že je podnikatelem, uzavírá smlouvu při svém podnikání, a na smlouvu se tudíž neuplatní ustanovení § 1793 občanského zákoníku.

XIII.10. Pro účely doručování písemností platí domněnka doby dojití tak, že při neúspěšném doručení do sídla smluvní strany držitelem poštovní licence se písemnost považuje za doručenou uplynutím třetího pracovního dne ode dne odeslání.

XIII.11. Tato smlouva je uzavřena dnem jejího podpisu smluvní stranou, která přijala nabídku – návrh na uzavření smlouvy. Smlouva nabude účinnosti uveřejněním v registru smluv podle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů.

XIII.12. Smluvní strany berou na vědomí, že společnost STAREZ – SPORT, a.s., je osobou povinnou uveřejňovat smlouvy v registru smluv, a to právnickou osobou dle § 2 odst. 1 písm. n) zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (dále jen „zákon o registru smluv"). Smluvní strany proto souhlasí s tím, že společnost STAREZ – SPORT, a.s. je oprávněna uveřejnit celý obsah této smlouvy, a to i strojově čitelnou kopii stejnopisu smlouvy.

XIII.13. Smluvní strany shodně prohlašují, že si smlouvu před jejím podpisem přečetly a dohodly se o celém jejím obsahu, což stvrzují svými podpisy.

V Brně dne …….	V Brně dne ……
……..	……..
za objednatele	za zhotovitele
Mgr. Martin Mikš, generální ředitel	……..
STAREZ – SPORT, a.s.	……..