FAKULTNÍ NEMOCNICE OSTRAVA

ev. č. FNO: 002/OVZ/16/048-OD
OŘN-22/15

DODATEK Č. 1 KE SMLOUVĚ O ZAJIŠTĚNÍ ÚDRŽBY, PODPORY A ROZVOJE ze dne 26.9.2016

Fakultní nemocnice Ostrava,
17. listopadu 1790/5, 708 52 Ostrava – Poruba,
IČ: 00843989,
DIČ: CZ00843989,
Jednající: MUDr. Jiří Havrlant, MHA, ředitel
(dále jen **„Objednatel"**)
a
TIS Brno, s.r.o.
Sídlo: Křtiny 221, Křtiny 679 05
IČ: 26938944
Jednající: Ing. Tomáš Lejdar, jednatel
zapsaná v obchodním rejstříku vedeném Krajským soudem v Brně, oddíl C, vložka 46968
(dále jen „poskytovatel")

I. ZMĚNY

1. Na základě požadavku poskytovatele v souladu s čl. 4.6. smlouvy se smluvní strany dohodly na navýšení ceny dle Přílohy č. 1 o 13,4%. Roční cena služby uvedená v příloze č. 1 se tak navyšuje na 612.360 Kč bez DPH.

2. Objednatel požaduje rozšíření plnění o požadavky kybernetické bezpečnosti, které jsou uvedeny v Příloze tohoto dodatku a stávají se novou přílohou č. 4 Smlouvy. Poskytovatel se zavazuje postupovat v souladu s požadavky této přílohy.

3. S ohledem na rozšíření povinností Poskytovatele se strany dohodly na navýšení měsíční platby o 12.000,- Kč bez DPH a tedy i roční ceny služeb dle Přílohy č. 1 na 756.360 Kč bez DPH.

4. článek 4.1. nově zní:

„4.1. Cena za služby podle paragrafu 3.1. až 3.5. je 63.030 Kč bez DPH měsíčně, v případě neplnění parametrů služeb je cena krácena."

II. ZÁVĚREČNÁ USTANOVENÍ

1. Smluvní strany souhlasí, že Dodatek č. 1 bude zveřejněn dle zákona č. 340/2015 Sb., o registru smluv (dále jen „**Registr smluv**").
2. Dodatek č. 1 se stává platným podpisem obou Smluvních stran a účinným dne 1.11.2022, nejdříve však dnem zveřejnění v Registru smluv.
3. Ostatní ujednání Smlouvy nedotčená Dodatkem č. 1 zůstávají v platnosti a účinnosti.
4. Dodatek č. 1 je vyhotoven ve dvou stejnopisech s platností originálu, z nichž každá strana obdrží po jednom.

FAKULTNÍ NEMOCNICE OSTRAVA

ev. č. FNO: 002/OVZ/16/048-OD
OŘN-22/15

V Ostravě dne _____

MUDr. Jiří Havrlant
Digitálně podepsal MUDr. Jiří Havrlant
Datum: 2022.11.16 15:56:58 +01'00'

Fakultní nemocnice Ostrava
MUDr. Jiří Havrlant, MHA, ředitel

V Brně dne _____

Digitally signed by Ing. Tomáš Lejdar
Date: 2022.11.02 14:13:52 CET

TIS Brno, s.r.o.
Ing. Tomáš Lejdar, jednatel

Příloha Dodatku č. 1 – tj. nová Příloha č. 4 smlouvy

Příloha č. 4: Technická a organizační opatření (požadavky na kybernetickou bezpečnost)

Vzhledem k určení Fakultní nemocnice Ostrava (dále také „Objednatel") jako povinné osoby podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů, je Poskytovatel, kterého Objednatel určil jako Významného dodavatele podle § 2, písm. n) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) (dále také vyhláška č. 82/2018 Sb.), povinen zajistit součinnost při plnění požadavků vycházejících z tohoto zákona a z prováděcího právního předpisu vyhlášky o kybernetické bezpečnosti.

I. Ustanovení o bezpečnosti informací

1. Poskytovatel je při plnění Smlouvy povinen:
   a) mít vedenou evidenci osob podílejících se na plnění předmětu Smlouvy v HelpDesk systému Poskytovatele (dále také „HelpDesk") dostupném na internetové adrese https://bugs.tis-brno.cz/. K tomuto seznamu musí Poskytovatel umožnit Objednateli přístup, min. osobě zastávající roli Manažera kybernetické bezpečnosti Objednatele. Kontaktní údaje Manažera kybernetické bezpečnosti Objednatele jsou uvedeny na konci tohoto dodatku.
   b) rozvíjet bezpečnostní povědomí svých pracovníků, kteří se podílejí na plnění předmětu Smlouvy, informovat je o aktuálním plnění předmětu Smlouvy. Všichni pracovníci Poskytovatele, kteří se podílí na plnění předmětu Smlouvy musí být prokazatelně seznámeni s bezpečnostními požadavky Objednatele týkající se plnění předmětu Smlouvy. V případě, že Objednatel bude vyžadovat absolvování školení formou e-learningu určeného pro dodavatele, je Poskytovatel povinen zajistit jeho absolvování všemi osobami uvedenými v evidenci osob podle bodu a). Školení musí být prováděno v intervalu alespoň 1x ročně. Evidence o absolvovaném školení vede Poskytovatel v HelpDesku, v případě, že je školení zajišťováno ze strany Objednatele, tuto evidenci vede Objednatel.
   c) zajistit dostatečnou zastupitelnost klíčových pracovníků podílejících se na plnění předmětu Smlouvy, alespoň v rozsahu následujících rolí:
      - Projektový manažer
      - Konzultant/Analytik
      - Programátor
   d) zajistit potřebnou součinnost Objednateli při provádění aktualizace povinné bezpečnostní dokumentace podle zákona a vyhlášky o kybernetické bezpečnosti související s plněním předmětu Smlouvy.

2. Pracovníci Poskytovatele mohou vstupovat do prostředí Objednatele výhradně pomocí zabezpečeného VPN připojení, na základě podepsané dohody o vzdáleném přístupu do FNO a v souladu s ní.

3. K servisním zásahům nebo kontrole informačního systému smí Poskytovatel používat pouze počítač, který disponuje výrobcem podporovaným operačním systémem a má provedeny veškeré dostupné aktualizace tohoto systému.

4. Poskytovatel má zákaz provádět pokusy o neautorizovaný přístup ke zdrojům Objednatele a má zákaz realizovat pokusy o neoprávněnou modifikaci nebo jiné neoprávněné zásahy do prostředků Objednatele.

5. Pracovníci Poskytovatele mají přístup výhradně k prostředkům (zejména servery) souvisejícím s plněním předmětu Smlouvy, ke kterým jim Poskytovatel umožnil přístup.

6. Poskytovatel je povinen provádět pravidelně aktualizace operačního systému včetně databáze dodávaného SW a ostatních podpůrných komponent minimálně 1x měsíčně nebo neprodleně po zveřejnění zneužitelných zranitelností. Pokud pro aktualizaci bude nutný restart operačního systému nebo aplikace, plánovaný termín výpadku bude předložen Objednateli ke schválení. Poskytovatel je povinen instalovat aktualizace pouze v případě, že byly řádně otestovány Poskytovatelem ve svém testovacím prostředí a na základě výsledků testování jsou považovány za použitelné.

7. Poskytovatel je oprávněn vstupovat do režimových prostor Objednatele pouze po předchozí domluvě a pod dohledem oprávněného pracovníka Objednatele, kterého určí Objednatel.

II. Ustanovení o oprávnění užívat data

1. Poskytovatel je povinen se všemi informacemi získanými při poskytování služeb dle Smlouvy nakládat pouze v rozsahu nezbytném pro plnění předmětu Smlouvy a v souladu se Smlouvou a právními předpisy České republiky.

2. Poskytovatel je povinen dodržovat zákaz kopírování a sdělování informací mimo Objednatele dalším subjektům. Předání jakýchkoliv dat a informacím třetím stranám je možné pouze po vzájemné dohodě smluvních stran. Poskytovatel je oprávněn předat data a informace nezbytné pro plnění Smlouvy svým poddodavatelům.

3. Data ukládána na datových nosičích u Poskytovatele, která budou obsahovat osobní data pacientů ve smyslu GDPR a zákona č. 110/2019 Sb. o ochraně osobních údajů, ve znění pozdějších předpisů, musí být šifrována.

III. Ustanovení o autorství programového kódu, popřípadě o programových licencích

1. Poskytovatel je povinen reagovat na žádost Objednatele o změnu zdrojového kódu. Reakcí Dodavatele se rozumí vyjádření se k požadavku Objednatele a posouzení požadované změny. Další postup je potom stanoven na základě dohody obou smluvních stran.

IV. Ustanovení o kontrole a auditu dodavatele (pravidla zákaznického auditu)

1. Objednatel má právo v pravidelných intervalech provádět u Poskytovatele průběžnou kontrolu dodržování bezpečnostních požadavků Objednatele souvisejících s předmětem plnění předmětu Smlouvy. Plánovanou kontrolu Objednatel oznámí Poskytovateli v dostatečném předstihu, tj. min. měsíc před plánovanou kontrolou. Poskytovatel má právo vykonávat kontrolu max. jednou za 1 rok nebo v návaznosti na závažné změny (např. po proběhlém kybernetickém bezpečnostním incidentu), které mohou mít vliv na plnění Smlouvy. Max. rozsah auditu kontroly je 1 pracovní den. Náklady na provedení auditu se zavazuje hradit výhradně Objednatel (zejména v případě, že se Objednatel rozhodne provedení auditu třetí stranou).

2. Předmětem kontroly může být:

   a) kontrola zařízení, ze kterých je vstupováno do prostředí Objednatele spočívající v kontrole verze operačního systému a provádění pravidelných aktualizací.
   b) kontrola nosičů, na kterých jsou uchovávána data související s předmětem plnění Smlouvy,
   c) dokumentace související s plněním předmětu Smlouvy a s plněním bezpečnostních požadavků Objednatele (např. deklarace plnění bezpečnostních požadavků u pracovníků podílejících se na plnění předmětu Smlouvy),
   d) vstup do prostor, které souvisí s plněním předmětu Smlouvy,
   e) naplnění předaných bezpečnostních požadavků souvisejících s plněním předmětu Smlouvy.

3. Rozsah a předmět kontroly bude šetřit práva a další obchodní činnost Objednatele. Kontrola bude vždy probíhat pouze v rozsahu nezbytně nutném ke kontrole povinností Poskytovatele podle Smlouvy.

4. Poskytovatel je povinen zajistit dostatečnou součinnost Objednateli při provádění kontroly.

5. V případě, že Objednatel při provádění kontroly zjistí nedostatky, je Poskytovatel povinen učinit kroky k jejich nápravě, a informovat Objednatele o provedených nápravných opatření.

6. Kontrola musí být provedena tak, aby nenarušila integritu, důvěrnost a dostupnost dat Poskytovatele, jakož i jeho obchodní tajemství a podnikatelskou činnost.

7. V případě, že je Poskytovatel držitelem certifikace ISO 27001, anebo jsou u Poskytovatele prováděny interní audity kybernetické bezpečnosti, lze článek IV. tohoto dodatku nahradit doložením zprávy z pravidelného auditu ISO 27001, popř. interního auditu kybernetické bezpečnosti.

V. Ustanovení upravující řetězení dodavatelů

1. V případě, že Poskytovatel bude k plnění předmětu Smlouvy využívat poddodavatele, je Poskytovatel povinen poddodavatele smluvně zavázat k dodržování povinností minimálně v rozsahu, v jakém je k nim povinen Poskytovatel podle této Smlouvy.

VI. Ustanovení o řízení změn

1. V případě potřeby změn týkajících se plnění předmětu Smlouvy, musí být vždy Objednatelem a Poskytovatelem předem projednány a odsouhlaseny oběma stranami a zaevidovány v HelpDesku. Poskytovatel je povinen reagovat na požadované změny ze strany Objednatele. Tímto ustanovením není dotčena povinnost smluvních stran uzavřít dodatek ke Smlouvě zohledňující změny Smlouvy.

2. Poskytovatel je povinen řídit změny, zejména určovat významné změny v rozsahu § 11 vyhlášky č. 82/2018 Sb., které by mohly mít vliv na plnění předmětu Smlouvy, přičemž je povinen na žádost Objednatele informovat o výsledcích řízení změn a přijmout nezbytná opatření k eliminaci možných nepříznivých dopadů na plnění předmětu Smlouvy.

Dle vyhlášky č. 82/2018 Sb., je významnou změnou změna, která má nebo může mít vliv na kybernetickou bezpečnost a představuje vysoké riziko

VII. Informační povinnost Poskytovatele

1. Poskytovatel je povinen vést aktualizovaný seznam aktiv, která spadají do rozsahu plnění předmětu Smlouvy (vzor seznamu aktiv je uveden na konci této přílohy).

2. Poskytovatel je povinen řídit rizika spojená s plněním předmětu Smlouvy, tj. Poskytovatel musí:

   a) identifikovat a hodnotit rizika v souvislosti s plněním předmětu Smlouvy (při hodnocení rizik je doporučeno vycházet z přílohy č. 2 vyhlášky č. 82/2018 Sb.), při hodnocení rizik lze využít standardní metody založené na součinu Riziko = dopad * hrozba * zranitelnost (Riziko je možnost, že určitá hrozba využije zranitelnosti a způsobí škodu). Hodnotící tabulky je možné nalézt v příloze vyhlášky č. 82/2018 Sb.

   b) na základě výsledků hodnocení rizik, zavést vhodná bezpečnostní opatření, monitorovat je a vyhodnocovat jejich účinnost (opatření musí být navrhovány i s ohledem na možné dopady na práva a povinnosti subjektů údajů).

   c) hodnocení rizik provádět alespoň 1x za 3 roky, a v případě výskytu závažného incidentu typu havárie vždy, typu porucha s ohledem na dopady nebo významné změny (např. změna konfigurace), která by mohla mít vliv na poskytování předmětu Smlouvy. V případech uvedených v tomto odstavci, výsledky hodnocení rizik budou zaevidovány v rámci řešení požadavku v aplikaci HelpDesk.

   d) na žádost Objednatele informovat Objednatele o způsobu řízení rizik a o zbytkových rizicích souvisejících s plněním předmětu Smlouvy.

   e) zajistit potřebnou součinnost při provádění hodnocení rizik ze strany Objednatele. Pokud Objednatel identifikuje riziko, jehož míra převyšuje stanovenou akceptovatelnou úroveň v podmínkách Objednatele a souvisí s plněním předmětu Smlouvy, Objednatel informuje bez zbytečného odkladu Poskytovatele a Poskytovatel je povinen spolupracovat na stanovení vhodných bezpečnostních opatření ke snížení tohoto rizika a zajistit přijetí opatření na své straně přiměřených předmětu Smlouvy a jeho činnostem podle Smlouvy.

3. Poskytovatel je povinen monitorovat zranitelnosti informačního systému a konfigurační nesoulady, neprodleně informovat Objednatele o těchto zjištěných skutečnostech a spolupracovat při jejich řízení.

4. V případě vzniku incidentu na straně Poskytovatele, který může mít vliv na plnění předmětu Smlouvy, je Poskytovatel povinen neprodleně informovat Objednatele včetně poskytnutí informací o řešení incidentu.

5. Poskytovatel je povinen informovat neprodleně Manažera kybernetické bezpečnosti Objednatele o významné změně ovládání Dodavatele podle zákona č. 90/2012, o obchodních korporacích, ve znění pozdějších předpisů nebo změny vlastnictví zásadních aktiv nebo změně oprávnění nakládat s těmito aktivy využívanými Dodavatelem k plnění předmětu Smlouvy.

VIII. Specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy

1. V případě výpovědi Smlouvy, je Poskytovatel povinen během výpovědní lhůty zpracovat plán, který bude stanovovat postupy pro případ ukončení Smlouvy (migrace dat, zajištění podpory v době přechodu na nové řešení apod.). Plán po zpracování předložit Manažerovi kybernetické bezpečnosti Objednatele ke kontrole a odsouhlasení.

IX. Specifikace podmínek pro řízení kontinuity činností

1. Poskytovatel musí mít zajištěnou kontinuitu činností, aby byl schopen zajišťovat plnění předmětu Smlouvy.

2. V případě vzniku mimořádné situace související s plněním předmětu Smlouvy, je Poskytovatel povinen určit osobu, která bude součástí „Týmu obnovy FNO". Jméno osoby je povinen sdělit Manažerovi kybernetické bezpečnosti Objednatele do 15 dní od podpisu tohoto dodatku. Osoba musí být schopna zastat roli Konzultanta/Analytika nebo Programátora podle Smlouvy. Osoba bude povinna plnit pokyny Manažera kybernetické bezpečnosti Objednatele směřující k vyřešení mimořádné situace do vyřešení dané situace. V případě, že řešení mimořádné situace, u které bude nezbytná účast Poskytovatele, překročí dobu 2 člověkodnů, má Poskytovatel právo si naúčtovat vícepráce podle ceníku prací uvedených v příloze č. 2 Smlouvy.

3. Poskytovatel musí umožnit Objednateli provedení bezpečnostního testování dodaného informačního systému, případně návazných podpůrných komponent, včetně testování kontinuity v předem stanovených termínech a zajistit Objednateli případnou součinnost (zejména navrácení do původního stavu).

4. Poskytovatel musí provádět nepřetržitý provozní monitoring aplikace a operačního systému za účelem včasné reakce Poskytovatele na události, které by vedly ke snížení dostupnosti aplikace např. z důvodu nedostatku systémových zdrojů, nefunkčnosti komponent informačního nebo operačního sytému apod., jedná se zejména o monitoring:

   a) **všech serverů:** kontrola místa na disku, kontrola přetečení inodes,

   b) **produkčních databázových serverů:** kontrola správné funkce zrcadlení, dostupnost a korektní odezva (test funkčnosti),

   c) **aplikačního serveru:** dostupnost a korektní odezva aplikace, funkčnost serverové části internetového objednávání, kontrola periodicky spouštěných úloh,

   d) **serveru pro internetové objednávání:** kontrola dostupnosti a korektní funkce internetového objednávání.

5. Poskytovatel je povinen provést a udržovat instalaci databázových serverů v režimu vysoké dostupnosti active-passive. Agent zálohující databázi bude provozován pouze na aktivním nodu clusteru, proto aktivní node musí mít nastavenu nejvyšší prioritu, aby zůstal vždy aktivním nodem.

6. Poskytovatel je povinen vypracovat plán zálohování zajišťující aplikační konzistenci prováděných záloh, který bude využívat stávající zálohovací systém Objednatele a který bude vyhovovat požadovaným časům:

   a) Servery: RPO 24 hod. a RTO 2 hod.

   b) Databáze postgreSQL: RPO: 1 hod. a RTO: 2 hod.

X. Specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání správcem

1. Poskytovatel je povinen předat či zničit uchovávaná data (informace) na požádání Objednatele během trvání smluvního vztahu, respektive vždy při jeho ukončení. To neplatí, pokud je Poskytovatel povinen data uchovávat podle závazných právních předpisů.

2. V případě předání dat, provozních údajů a informací bude formát těchto dat/údajů/informací v případě potřeby dohodnut individuálně mezi Objednatelem a Poskytovatelem; vždy však musí být v souladu s doporučenými formáty Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB).

3. V případě potřeby likvidace dat a technických nosičů informací, které mohou obsahovat data Objednatele, musí Poskytovatel postupovat v souladu s přílohou č. 4 vyhlášky č. 82/2018 Sb., úroveň důležitosti aktiva Vysoká.

XI. Ustanovení o právu jednostranně odstoupit od smlouvy

1. Objednatel má dále právo jednostranně odstoupit od Smlouvy v případě významné změny podle vyhlášky č. 82/2018 Sb., kontroly nad Dodavatelem podle zákona č. 90/2012, o obchodních korporacích, ve znění pozdějších předpisů nebo změny vlastnictví zásadních aktiv nebo změně oprávnění nakládat s těmito aktivy využívanými Poskytovatelem k plnění předmětu Smlouvy.

XII. Napojení na management bezpečnostních informací a událostí (SIEM)

1. V případě potřeby Objednatele napojení informačního systému na management bezpečnostních informací a událostí (SIEM) se Poskytovatel zavazuje na základě tohoto dodatku zajistit odesílání požadovaných aplikačních událostí protokolem Syslog do systému SIEM provozovaného Objednatelem. Minimální předpokládaný rozsah předávaných údajů:

a) datum a čas včetně specifikace časového pásma,

b) typ činnosti,

c) identifikaci technického aktiva, které činnost zaznamenalo,

d) jednoznačnou identifikaci účtu, pod kterým byla činnost provedena,

e) jednoznačnou síťovou identifikaci zařízení původce,

f) úspěšnost nebo neúspěšnost činnosti,

g) přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů,

h) činností provedených administrátory,

i) úspěšné i neúspěšné manipulace s účty, oprávněními a právy,

j) neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,

k) činností uživatelů, které mohou mít vliv na bezpečnost informačního systému,

l) zahájení a ukončení činností technických aktiv,

m) kritických i chybových hlášení technických aktiv a

n) přístupů k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí.

XIII. Ostatní ujednání

V případě potřeby integrace informačního systému k jinému informačnímu systému, se Poskytovatel zavazuje na základě cenové nabídky a následné objednávky zajistit dostatečnou součinnost Objednateli.

Kontaktní údaje Objednatele

Označení role	Jméno a příjmení	Kontaktní údaje (tel., e-mail)
Manažer kybernetické bezpečnosti Fakultní nemocnice Ostrava	[redacted]	[redacted]

VZOR SEZNAMU AKTIV

Popis aktiva	**Označení typového aktiva**	**Kategorie aktiva (služby, informace a data, technické aktivum, zaměstnanci, dodavatelé)**	**Specifikace (HW, SW, objekt, vývojový pracovník apod.):**
Provozní data	T-001 Provozní data	Informace	---
Zaměstnanci TIS TRATIS	T-002 Zaměstnanci TIS	Zaměstnanci	Vývojový pracovník SW