FAKULTNÍ NEMOCNICE OSTRAVA

ev. č. FNO: 002/OVZ/21/170-K, OŘN- 23/21
ev. číslo Dodavatele: SML-2021-2275

DODATEK Č. 1 KE SMLOUVĚ O DODÁVCE, IMPLEMENTACI A PODPOŘE SYSTÉMU PACS ze dne 16. 11. 2021

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
OR-CZ spol. s r.o.
sídlo: Gorazdova 1477/2, Předměstí, 571 01 Moravská Třebová
IČ: 48168921
DIČ: CZ48168921 (je plátcem DPH)
zapsaná v obchodním rejstříku vedeném u Krajského soudu v Hradci Králové, oddíl C, vložka 4090
jednající: Ing. Václav Mačát, jednatel
(dále jen „**Dodavatel**")

I. ZMĚNY

1. 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, se rozšiřují povinnosti Dodavatele o požadavky kybernetické bezpečnosti, které jsou uvedeny v Příloze tohoto dodatku a stávají se novou přílohou č. 5 Smlouvy. Dodavatel se zavazuje postupovat v souladu s požadavky této přílohy.

II. ZÁVĚREČNÁ USTANOVENÍ

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

V Ostravě dne _____

MUDr. Jiří Havrlant
Digitálně podepsal MUDr. Jiří Havrlant
Datum: 2022.12.28 14:15:06 +01'00'

Fakultní nemocnice Ostrava
MUDr. Jiří Havrlant, MHA, ředitel

V Moravské Třebové dne _____

Ing. Václav Mačát
Digitálně podepsal Ing. Václav Mačát
Datum: 2022.12.15 12:38:52 +01'00'

OR-CZ spol. s r.o.
Ing. Václav Mačát

Příloha č. 5: 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 (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, je Dodavatel, 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), 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. Dodavatel je při plnění Smlouvy povinen:
   a) mít vedenou evidenci osob podílejících se na plnění předmětu Smlouvy v HelpDesk systému Dodavatele (dále také „Helpdesk") dostupném na internetové adrese https://servicedesk.orcz.cz/. K tomuto seznamu musí Dodavatel 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 Dodavatele, 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 Dodavatel povinen zajistit jeho absolvování všemi osobami uvedenými v evidenci osob podle bodu a). Školení musí být prováděno v intervalu alespoň 1x ročně a školení bude max. v rozsahu 1-2 hod. / rok. Evidence o absolvovaném školení vede Dodavatel 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:
      - Technický specialista
   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 Dodavatele 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 Dodavatel používat pouze počítač, který je vybaven výrobcem podporovaným operačním systémem, antivirovým programem s aktuální virovou databází a má provedeny veškeré dostupné aktualizace tohoto systému.

4. Dodavatel 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 Dodavatele mají přístup výhradně k prostředkům (zejména servery) souvisejícím s plněním předmětu Smlouvy, ke kterým jim Dodavatel umožnil přístup.

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

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

3. Data ukládána na datových nosičích u Dodavatele, 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. Dodavatel 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 Dodavatele průběžnou kontrolu dodržování bezpečnostních požadavků Objednatele souvisejících s předmětem plnění předmětu Smlouvy. Plánovanou kontrolu Objednatel oznámí Dodavateli v dostatečném předstihu, tj. min. měsíc před plánovanou kontrolou. Dodavatel má právo vykonávat audit kontrolu max. jednou za 2 roky 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 pro 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, antivirové ochrany a provádění pravidelných aktualizací,
   b) kontroly 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, tj. do prostor organizace Dodavatele, ve kterých dochází k plnění 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 Dodavatele podle Smlouvy.

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

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

6. Audit/Kontrola musí být proveden/a tak, aby nenarušil/a integritu, důvěrnost a dostupnost dat Dodavatele, jakož i jeho obchodní tajemství a podnikatelskou činnost.

7. V případě, že je Dodavatel držitelem certifikace ISO 27001, anebo jsou u Dodavatele 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 Dodavatel bude k plnění předmětu Smlouvy využívat poddodavatele, je Dodavatel povinen poddodavatele smluvně zavázat k dodržování povinností minimálně v rozsahu, v jakém je k nim povinen Dodavatel podle této Smlouvy. V případě, že poddodavatel bude zároveň poskytovatel/dodavatel Objednatele, a Objednatel bude vyžadovat součinnost poskytovatelů/dodavatelů, odpovědnost za dodržování povinností nese Objednatel.

VI. Ustanovení o řízení změn

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

2. Dodavatel je povinen řídit změny, zejména určovat významné změny v rozsahu § 11 vyhlášky o kybernetické bezpečnosti, 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 Dodavatele

1. Dodavatel je povinen vést aktualizovaný seznam aktiv, která spadají do rozsahu plnění předmětu Smlouvy.

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

   a) identifikovat a hodnotit rizika v souvislosti s plněním předmětu Smlouvy (při hodnocení rizik je doporučeno vycházet z přílohy č. 2 vyhlášky o kybernetické bezpečnosti, 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 této vyhlášky.

   b) na základě výsledků hodnocení rizik, zavést vhodná bezpečnostní opatření, monitorovat je a vyhodnocovat jejich účinnost (opatření musí být navrhována 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 plnění předmětu Smlouvy,

   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 Dodavatele a Dodavatel 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. Dodavatel 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 Dodavatele, který může mít vliv na plnění předmětu Smlouvy, je Dodavatel povinen neprodleně informovat Manažera kybernetické bezpečnosti Objednatele včetně poskytnutí informací o řešení incidentu.

5. Dodavatel 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 Dodavatel 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. Dodavatel musí mít zajištěnou kontinuitu činností, aby byl schopen zajišťovat plnění předmětu Smlouvy.

2. V případě vzniku mimořádné situace související s plněním předmětu Smlouvy, je Dodavatel 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 Technického specialisty podle Smlouvy. Dodavatel může dodat jména více osob. 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 Dodavatele, v případě, že mimořádnou situaci způsobil Objednatel, překročí dobu 2 člověkodnů, má Dodavatel právo si naúčtovat vícepráce podle ceníku prací uvedených v příloze č. 2 Smlouvy.

3. Dodavatel 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. Dodavatel musí provádět nepřetržitý provozní monitoring aplikace a operačního systému za účelem včasné reakce Dodavatele 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:** na úrovni OS a virtuálního HW,

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

   c) **aplikačního serveru:** dostupnost a korektní odezva aplikace, kontrola periodicky spouštěných úloh.

5. Dodavatel je povinen vypracovat plán zálohování zajišťující aplikační konzistenci prováděných záloh, který bude využívat stávající zálohovací systém Objednatele.

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

1. Dodavatel je povinen předat či zničit uchovávaná data (informace) na požádání Objednatele během trvání smluvního vztahu, respektive vždy při jeho ukončení. To neplatí, pokud je Dodavatel 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 Dodavatelem; 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 Dodavatel postupovat v souladu s přílohou č. 4 vyhlášky o kybernetické bezpečnosti, úroveň důležitosti aktiva Vysoká.

XI. Ustanovení o právu jednostranně odstoupit od smlouvy

1. Objednatel má dále právo jednostranně odstoupit od Smlouvy podle vyhlášky o kybernetické bezpečnosti v případě významné změny 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 Dodavatelem 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 Dodavatel zavazuje, že informační systém umožní zaznamenávání bezpečnostních a provozních událostí a odesílání požadovaných událostí do 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

1. V případě potřeby integrace informačního systému k jinému informačnímu systému, se Dodavatel zavazuje na základě cenové nabídky a následné objednávky podle bodu 3.6 Smlouvy zajistit dostatečnou součinnost Objednateli.

2. Podmínky poskytnutí veškeré výše uvedené součinnosti Dodavatele, které nejsou součástí plnění předmětu Smlouvy, budou mezi oběma smluvními stranami stanoveny vždy individuálně na základě žádosti Objednatele. Dodavatel vždy stanoví pracnost a technické, časové, případně další podmínky pro provedení požadované součinnosti. Dodavatel má právo požadovanou součinnost odmítnout, pokud ji není schopen z technického či personálního důvodu zajistit.

Kontaktní údaje Objednatele

Označení role	[redacted]
Manažer kybernetické bezpečnosti Fakultní nemocnice Ostrava	

SEZNAM ZRANITELNOSTÍ A HROZEB (podle vyhlášky o kybernetické bezpečnosti)

Zranitelnosti

1. nedostatečná údržba informačního a komunikačního systému,
2. zastaralost informačního a komunikačního systému,
3. nedostatečná ochrana vnějšího perimetru,
4. nedostatečné bezpečnostní povědomí uživatelů a administrátorů,
5. nedostatečná údržba informačního a komunikačního systému,
6. nevhodné nastavení přístupových oprávnění,
7. nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
8. nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování,
9. nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí,
10. nedostatečná ochrana aktiv,
11. nevhodná bezpečnostní architektura,
12. nedostatečná míra nezávislé kontroly,
13. neschopnost včasného odhalení pochybení ze strany zaměstnanců.

Hrozby

1. porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,
2. poškození nebo selhání technického anebo programového vybavení,
3. zneužití identity,
4. užívání programového vybavení v rozporu s licenčními podmínkami,
5. škodlivý kód (například viry, spyware, trojské koně),
6. narušení fyzické bezpečnosti,
7. přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie,
8. zneužití nebo neoprávněná modifikace údajů,
9. ztráta, odcizení nebo poškození aktiva,
10. nedodržení smluvního závazku ze strany dodavatele,
11. pochybení ze strany zaměstnanců,
12. zneužití vnitřních prostředků, sabotáž,
13. dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb,
14. nedostatek zaměstnanců s potřebnou odbornou úrovní,
15. cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik,
16. zneužití vyměnitelných technických nosičů dat,
17. napadení elektronické komunikace (odposlech, modifikace).