Dodatek č. 1

ke Smlouvě o dodávce IT služeb

Smluvní strany:

Fakultní nemocnice v Motole,

státní příspěvková organizace, zřízená Ministerstvem zdravotnictví ČR

se sídlem: V Úvalu 84, 150 06 Praha 5 - Motol

IČ: 00064203, DIČ: CZ00064203

zastoupená:

na straně jedné jako objednatel (dále také jen „**Objednatel**")

a

Kancelářské stroje s.r.o.

se sídlem: Dykova 1068/9, 101 00 Praha 10 - Vinohrady

IČ: 26467658, DIČ: CZ26467658

zastoupen:

zapsána v obchodním rejstříku vedeném Městským soudem v Praze, sp. zn. C 84203,

na straně druhé jako poskytovatel (dále jen "**Poskytovatel**")

uzavírají tento dodatek č. 1:

I. ÚČEL A PŘEDMĚT DODATKU

Účelem dodatku je v souladu s ustanovením § 4 odst. 4 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění (dále jen „**ZoKB**"), ve spojení s přílohou č. 7 k vyhlášce 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), v platném znění (dále jen „**Vyhláška**"), stanovit závazná bezpečnostní opatření, která se vztahují na Poskytovatele.

Předmětem dodatku je změna a doplnění Smlouvy o poskytování IT služeb ze dne 27.5.2008 (dále jen „**Smlouva")** týkající se poskytování plnění Poskytovatele, které je (výhradně či jako součást předmětu plnění jiné služby) součástí vývoje, dodávek, implementace a/nebo servisu software či hardware (dále také jen „**SW**" či „**HW**"), a/nebo který v souvislosti s plněním pro Objednatele přistupuje do informačního systému Objednatele, který byl určen informačním systémem základní služby (dále jen „**ISZS**")
v souladu se zákonem o kybernetické bezpečnosti, a/nebo který v rámci poskytovaného plnění pro Objednatele zpracovává, a/nebo přenáší a/nebo ukládá a/nebo archivuje data a provozní údaje Objednatele a/nebo jeho klientů / pacientů a osob jim blízkých a/nebo zabezpečuje dodávky HW komponent systému či má přístup k HW komponentám ISZS (dále také jen „**Bezpečnostní opatření**").

V důsledku toho smluvní strany mění a doplňují svá smluvní ujednání jak níže uvedeno.

II. DOPLNĚNÍ SMLOUVY

Dosavadní stávající znění ustanovení Smlouvy se doplňuje o práva a povinnosti stran sjednaných v tomto dodatku za účelem zavedení Bezpečnostních opatření.

1. POVINNOSTI POSKYTOVATELE PŘI PLNĚNÍ SMLOUVY:

1.1. postupovat v souladu s platnými právními předpisy, zejména pak se ZoKB a Vyhláškou a reflektovat případné novely uvedených právních předpisů či novou právní úpravu a postupovat v souladu objednávkami a dalšími požadavky Objednatele, jakožto správce a provozovatele informačního sytému základní služby.

2. pokud při plnění předmětu Smlouvy Poskytovatel zpracovává osobní údaje pro Objednatele, zavazuje se Poskytovatel uzavřít s Objednatelem smlouvu o zpracování osobních údajů v souladu se zákonem o zpracování osobních údajů č. 110/2019 Sb., (dále jen „**zákon o zpracování osobních údajů**") a nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

3. předmět plnění nesmí být nevyhovující z hlediska informační bezpečnosti, přičemž za nevyhovující je považováno jakékoli plnění, které obsahuje technologie/klíčové prvky, vůči jejichž výrobcům příslušný správní orgán vydal opatření v souladu se ZoKB, a které dle analýzy rizik představují vysoké riziko, případné změny plnění v souladu s předchozí větou budou uskutečněny Poskytovatelem na základě písemné objednávky Objednatele.

4. dodržovat příslušná ustanovení bezpečnostních politik, metodik a postupů Objednatele resp. platné řídící dokumentace Objednatele či její části, která jsou relevantní k předmětu plnění, pokud byl Poskytovatel s příslušnými dokumenty nebo jejich částmi prokazatelně seznámen.

5. zaznamenávat podstatné okolnosti související s poskytovaným předmětem plnění dle Smlouvy (technické záznamy, organizační záznamy o školení, pověření apod.) a informovat o nich Objednatele.

6. zabezpečit plnění povinností stanovených v tomto dodatku za účelem zajištění Bezpečnostních opatření popsaných v ustanoveních dále.

2. FYZICKÁ DOSTUPNOST A BEZPEČNOST INFORMACÍ

2.1. Poskytovatel se zavazuje dodržovat provozní řády budov, jednotlivých pracovišť (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny komponenty systémů ISZS anebo datové nosiče (dále také jen „**Pracoviště**").

2.2. Poskytovatel se zavazuje, že na Pracovišti neponechá volně dostupná instalační, záložní nebo archivní média ani dokumentaci k systému ISZS nebo k jeho HW komponentám,

které jsou předmětem plnění dle Smlouvy. HW komponentou se rozumí se každý HW prvek, který je nosičem dat ISZS, ukládá nebo třídí data ISZS a/nebo je ovládán SW, který je součástí ISZS.

3. PŘÍSTUP K INFORMACÍM

3.1. Poskytovatel bere na vědomí, že přístup k systému ISZS nebo k jeho HW komponentám je možné povolit pouze fyzické identitě zaměstnance Poskytovatele (popřípadě Poddodavatele) zaevidované v registru identit Objednatele, a to na základě požadavku Poskytovatele na přístup.

3.2. Poskytovatel bere na vědomí, že jeho zaměstnanec musí poskytnout své osobní údaje Objednateli, a to v rozsahu nutném pro zřízení přístupu. V opačném případě Objednatel není povinen přístup k systému ISZS nebo k jeho HW komponentám zaměstnanci Poskytovatele povolit. Zaměstnanec Poskytovatele s přiděleným přístupem (fyzickým, logickým) k systému ISZS nebo k jeho HW komponentám bere na vědomí, že dochází ke zpracování osobních údajů během vyhodnocování údajů o pohybu a prováděných aktivitách v prostorách Objednatele. Poskytovatel bere na vědomí, že přidělení oprávnění zaměstnanci Poskytovatele musí být řízeno principem nezbytného minima a není nárokové.

3.3. Poskytovatel se zavazuje, že udělený přístup nebude sdílen více zaměstnanci Poskytovatele nebo Poddodavatele.

3.4. Poskytovatel se zavazuje, že vzdálený přístup do systému ISZS nebo k jeho HW komponentám bude vždy uskutečněn pouze prostřednictvím zabezpečeného připojení VPN.

3.5. Poskytovatel se zavazuje, že před připojením koncového zařízení, mobilního koncového zařízení nebo aktivního síťového prvku jako síťové switche, WiFi access pointy, routery či huby do počítačové sítě zažádá o schválení připojení kontaktní osobu na straně Objednatele.

3.6. Poskytovatel se zavazuje, že bez zbytečného odkladu deaktivuje všechny nevyužívané zakončení sítě anebo nepoužívané porty aktivního síťového prvku, pokud daná činnost bude při plnění předmětu Smlouvy vyžadována.

3.7. Poskytovatel se zavazuje, že nebude instalovat a používat SW představující bezpečnostní riziko, zejména nástroje typu Keylogger, Sniffer, Analyzátor zranitelností a Port Scanner, Backdoor, rootkit a trojský kůň nebo jinou podobu malware.

3.8. Poskytovatel se zavazuje, že všechny jeho informační systémy, které se připojují do síťové infrastruktury Objednatele, jsou a budou chráněny proti malware nebo jiným formám škodlivého SW.

3.9. Poskytovatel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části systému ISZS nebo na jeho HW komponentách programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci systému ISZS nebo nelegální získání dat a informací, nebo má za cíl tyto činnosti usnadnit.

3.10. Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli v ISZS:

a) neukládaly, nesdílely, data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele,

b) nestahovaly, nesdílely, neukládaly, nearchivovaly a/nebo neinstalovaly datové a spustitelné soubory v rozporu s licenčními podmínkami nebo zákonem 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"),

c) nezasílaly řetězové emaily.

3.11. Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli, které přistupují do interní sítě nebo ISZS Objednatele, měly v externím zařízení typu notebook/počítač aplikovány bezpečnostní záplaty a nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu.

3.12. Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli, které přistupují do interní sítě a/nebo systému ISZS Objednatele chránily autentizační prostředky a údaje k systémům ISZS Objednatele. Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako kybernetická bezpečnostní událost ve smyslu příslušné řídící dokumentace a mohou být uplatněny příslušné postupy zvládání kybernetické bezpečnostní události (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu). Poskytovatel bere na vědomí, že postup zvládáním kybernetické bezpečnostní události či jiný důsledek porušení Bezpečnostních opatření nebude posuzován jako okolnost vylučující odpovědnost Poskytovatele za prodlení s řádným a včasným plněním předmětu Smlouvy a nebude důvodem k jakékoli náhradě případné újmy Poskytovateli či jiné osobě ze strany Objednatele.

3.13. Poskytovatel bere na vědomí, že veškerá jeho aktivita a jeho plnění realizované v systémovém prostředí Objednatele mohou být Objednatelem průběžně a pravidelně monitorovány a vyhodnocovány.

4. AUTORSTVÍ

4.1. Poskytovatel se při poskytování plnění pro Objednatele zavazuje zajistit, aby při plnění Smlouvy dodržel podmínky stanovené autorským zákonem.

5. OPRÁVNĚNÍ UŽÍVAT DATA

5.1. Poskytovatel je při poskytování plnění pro Objednatele oprávněn užívat data předaná Poskytovateli Objednatelem za účelem plnění předmětu Smlouvy, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu Smlouvy.

5.2. Poskytovatel se při poskytování plnění pro Objednatele zavazuje nakládat s daty pouze v souladu se Smlouvou a příslušnými právními předpisy, zejména ZoKB a Vyhláškou a dalšími souvisejícími právními předpisy.

6. ŘÍZENÍ ZMĚN, KONTINUITA ČINNOSTÍ

6.1. Objednatel v rámci řízení změn ISZS nebo jeho HW komponent přezkoumává možné dopady změn a určuje významné změny dle Vyhlášky. Poskytovatel je povinen spolupracovat s Objednatelem na řízení změn.

6.2. Objednatel u významných změn dokumentuje jejich řízení, provádí analýzu rizik, přijímá opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami, aktualizuje bezpečnostní politiku a bezpečnostní dokumentaci, zajistí testování ISZS, případně jeho HW komponent a zajistí možnost navrácení do původního stavu.

6.3. Objednatel má povinnost informovat Poskytovatele o výsledcích řízení změn, které mají dopady na plnění předmětu Smlouvy ze strany Poskytovatele.

6.4. Poskytovatel má povinnost přijmout účinná opatření ke snížení nepříznivých dopadů v souladu s výsledky řízení změn uvedených v čl. 6.3.

6.5. Poskytovatel se zavazuje poskytnout Objednateli veškerou nezbytnou součinnost při analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní dokumentace, souvisejícím testováním a zajištění možnosti navrácení do původního stavu.

6.6. V případě realizace penetračního testování nebo testování zranitelnosti řešení poskytne Poskytovatel Objednateli veškerou potřebnou součinnost.

6.7. Objednatel má oprávnění zapojit Poskytovatele do řízení kontinuity činností, a to zejména oprávnění k zahrnutí Poskytovatele do plánu kontinuity činností, který souvisí s ISZS nebo s jeho HW komponentami a souvisejících služeb a/nebo zahrnutí Poskytovatele do havarijního plánu Objednatele.

7. OZNAMOVACÍ A KONTROLNÍ POVINNOSTI SMLUVNÍCH STRAN

7.1. Poskytovatel má povinnost neprodleně informovat Objednatele o kybernetických bezpečnostních incidentech souvisejících s plněním předmětu Smlouvy. Součástí oznámení musí být popis povahy případu kybernetického bezpečnostního incidentu.

7.2. Poskytovatel má povinnost provést analýzu příčin kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování v případě, že Poskytovatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

7.3. Poskytovatel se zavazuje poskytnout Objednateli veškeré informace potřebné k doložení toho, že byly splněny povinnosti vyplývající z tohoto dodatku, jakož i ze ZoKB a Vyhlášky, a za tímto účelem se zavazuje umožnit Objednateli provedení kontrol, včetně auditů

prováděných Objednatelem či auditorem, kterého Objednatel k auditu pověří, a poskytne k těmto kontrolám a auditům veškerou potřebnou součinnost.

7.4. Poskytovatel je dále povinen umožnit provedení kontroly či auditu i ze strany dozorových orgánů.

7.5. Poskytovatel je povinen provádět v případech a termínech stanovených Vyhláškou vlastní hodnocení rizik a kontrolu zavedených bezpečnostních opatření. O způsobu řízení rizik a o rizicích souvisejících s plněním Smlouvy Poskytovatel podá Objednateli písemnou zprávu

7.6. Poskytovatel má povinnost bez zbytečného odkladu informovat Objednatele o významné změně ovládání Poskytovatele podle zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích) nebo změně vlastnictví základních aktiv, jakož i změně v oprávnění Poskytovatele nakládat s aktivy, která jsou využívána k plnění předmětu Smlouvy.

8. PODDODAVATELÉ

8.1. Poskytovatel nezapojí do poskytování plnění dle této Smlouvy žádného dalšího Poddodavatele bez předchozího písemného povolení Objednatele.

8.2. Poskytovatel se zavazuje, že se bude řídit požadavky Objednatele na řízení bezpečnosti informací a poskytne Objednateli veškerou nezbytnou součinnost v otázkách řízení bezpečnosti informací a pokud využívá při poskytování plnění Poddodavatele, zajistí, že bude Objednateli poskytnuta veškerá nezbytná součinnost v otázkách řízení bezpečnosti informací také od těchto Poddodavatelů.

8.3. Pokud Poskytovatel využívá za účelem plnění předmětu Smlouvy Poddodavatele, musí být tomuto Poddodavateli uloženy na základě smlouvy s Poskytovatelem stejné povinnosti k dodržování smluvních ujednání, jaká jsou sjednaná tímto dodatkem mezi Objednatelem a Poskytovatelem.

8.4. Poskytovatel má povinnost zajistit, že Poddodavatel bude v souladu s požadavky, které Objednatel ukládá na základě tohoto dodatku Poskytovateli.

Poskytovatel odpovídá za to, že jeho Poddodavatelé nebudou jednat v rozporu s bezpečnostními opatřeními vyplývajícími z tohoto dodatku, v případě, že dojde k nedodržení těchto požadavků ze strany Poddodavatele Poskytovatele, považuje se každé takové nedodržení požadavků za porušení povinnosti Poskytovatele dle Smlouvy.

9. OCHRANA DŮVĚRNÝCH INFORMACÍ

9.1. Strany se zavazují zachovat mlčenlivost o veškerých informacích, osobních údajích, datech či zprávách, o nichž se dozvěděly v souvislosti s přípravou či plněním této Smlouvy (dále jen „**důvěrné informace**"), a to včetně předmětu Smlouvy, vlastní spolupráce a vnitřních záležitostí Stran. Výjimkou ze zachování mlčenlivosti je plnění povinností Objednatele ve vztahu ke kontrolním orgánům vyplývající z obecně závazných právních předpisů

9.2. Strany se zavazují, že zajistí, aby se všechny osoby oprávněné zpracovávat důvěrné informace zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti. Závazek mlčenlivosti a ochrany důvěrných informací zůstává v platnosti i po ukončení této Smlouvy.

10. POVINNOSTI PŘI UKONČENÍ SMLOUVY

10.1. Poskytovatel se zavazuje poskytnout Objednateli veškerou potřebnou součinnost, dokumentaci a informace, účastnit se jednání s Objednatelem a popřípadě třetími osobami za účelem plynulého a řádného převedení všech činností spojených s provozem, servisem a rozvojem předmětu Smlouvy na Objednatele a/nebo nového poskytovatele, ke kterému dojde po skončení účinnosti této Smlouvy, a to vše dle pokynů Objednatele (dále jen „**Ukončení smlouvy**").

10.2. Poskytovatel se zavazuje poskytnout součinnost do doby přijetí a implementace nového řešení nebo jeho HW komponent v nezbytné míře tak, aby byla zachována funkčnost ISZS během přechodu na nové řešení, např. součinnost spočívající v migraci dat, podpory řešení atd.

11. SPECIFIKACE PODMÍNEK PRO PŘEDÁVÁNÍ INFORMACÍ

11.1. Za účelem zabezpečení přenosu dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost během poskytování plnění pro Objednatele ze strany Poskytovatele se dohodly strany takto:

Kontaktní osoby

	Fakultní nemocnice v Motole	**Kancelářské stroje s.r.o.**
Technická oblast	[redacted]	[redacted]
Kybernetická bezpečnost	[redacted]	[redacted]

formát předávání dat: _____
provozní údaje: _____
provozní informace: _____

12. PRAVIDLA PRO LIKVIDACI DAT

12.1. Poskytovatel se zavazuje poskytnout Objednateli veškerou potřebnou součinnost, pro likvidaci nepotřebných dat, za tím účelem smluvní strany dohodnou lhůty pro provádění likvidace dat, kde určí konkrétní rozsah a časové intervaly pro likvidaci dat. Smluvní strany

sjednávají, že k likvidaci dat přistoupí po vzájemném odsouhlasení likvidace, podmínky likvidace musí být v souladu Přílohou č. 4 Vyhlášky.

13. DŮSLEDKY PORUŠENÍ POVINNOSTI SMLUVNÍCH STRAN

13.1. Pro případ, že:

a) Poskytovatel nesplní informační povinnost stanovenou mu tímto dodatkem, nebo

b) dojde u Poskytovatele k významné změně kontroly nad osobou Poskytovatele, nebo

c) dojde u Poskytovatele ke změně kontroly nad zásadními aktivy Poskytovatele využívanými k plnění Smlouvy, nebo

d) Poskytoval, v rozporu s čl. II odst. 8.1, zapojí do plnění Smlouvy Poddodavatele bez písemného povolení Objednatele

je Objednatel oprávněn odstoupit od Smlouvy. Účinky odstoupení nastávají dnem doručení odstoupení od Smlouvy Poskytovateli. Odstoupení nezbavuje Poskytovatele povinnosti poskytnout součinnost dle ustanovení tohoto dodatku při Ukončení Smlouvy.

13.2. Pro případ porušení povinností Poskytovatele dle tohoto dodatku se sjednávají následující smluvní pokuty a sankce:

a) v případě nesplnění informační povinnosti stanovené tímto dodatkem Poskytovateli se sjednává smluvní pokuta ve výši 100.000,- Kč (slovy jednostotisíc korun českých) bez DPH za každé takové porušení,

b) v případě porušení některého z Bezpečnostních opatření sjednává se smluvní pokuta ve výši 500.000,- Kč (slovy pětsettisíc korun českých) bez DPH za každé takové porušení,

c) v případě neposkytnutí součinnosti po Ukončení smlouvy sjednává se smluvní pokuta ve výši 250.000,- Kč (slovy dvěstěpadesáttisíc korun českých) bez DPH.

13.3. Smluvní pokutou není dotčen nárok Objednatele na náhradu škody vzniklé v souvislosti s porušením smlouvy. Smluvní pokuta je splatná do 14 dní ode dne doručení uplatnění práva na smluvní pokutu Poskytovateli spolu s fakturou.

III. ZÁVĚREČNÁ USTANOVENÍ DODATKU

V ostatních ustanoveních zůstává Smlouva nadále beze změn. V případech, kdy tento Dodatek přímo nahrazuje práva a povinnosti vyplývající ze Smlouvy, se tato ustanovení Smlouvy ruší.

Tento dodatek je uzavírán v souladu s platnými právními předpisy České republiky. Pokud se jakékoli ustanovení tohoto dodatku stane neplatným či nevymahatelným, nebude to mít vliv na platnost a vymahatelnost ostatních ustanovení tohoto dodatku a rovněž Smlouvy. Strany se zavazují nahradit neplatné nebo nevymahatelné ustanovení novým ustanovením, jehož znění bude odpovídat úmyslu vyjádřenému původním ustanovením a tímto dodatkem jako celkem.

Ustanovení dodatku upravující Ukončení smlouvy, mlčenlivost nebo ochranu důvěrných informací, zůstávají platná a účinná i po skončení Smlouvy.

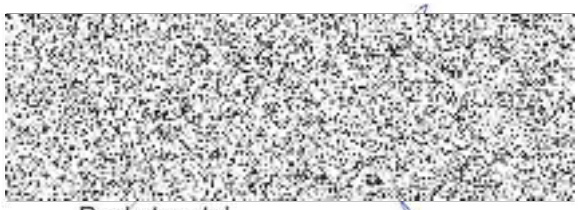
Dodatek je zpracován ve čtyřech vyhotoveních, z nichž dvě obdrží Objednatel a dvě Poskytovatel. Všechny vyhotovení dodatku mají stejnou platnost.

Dodatek nabývá platnosti dnem jeho podpisu a účinnosti v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv.

V Praze dne 13.3.2020

Objednatel

V Praze dne 9.3.2020



Poskytovatel