ICZ 859313 / 2

SMLOUVA O POSKYTOVÁNÍ SLUŽEB

uzavřená níže uvedeného dne, měsíce a roku podle ustanovení § 1746 odst. 2 zák. č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „**Smlouva**“) mezi níže uvedenými smluvními stranami:

Obchodní firma	Nemocnice Písek, a.s.
Se sídlem	Karla Čapka 589, Písek, 397 01
Zapsaná	Krajským soudem v Českých Budějovicích, oddíl B, vložka 1462
IČ	26095190
DIČ	CZ26095190
Zastoupená	MUDr. Jiřím Holanem, MBA, předsedou představenstva a Ing. Danou Čagánkovou, členkou představenstva
Bankovní spojení	20830271/0100, Komerční banka, a.s.

(dále jen „**Objednatel“**)

Obchodní firma	ICZ a.s.
Se sídlem	Na hřebenech II 1718/10, Nusle, 140 00 Praha 4
Zapsaná	v OR vedeném Městským soudem v Praze, oddíl B, vložka 4840
IČ	25145444
DIČ	CZ 699000372
Zastoupená	[redacted]
Bankovní spojení	

(dále jen „**Poskytovatel**“)

(Objednatel a Poskytovatel dále společně jako „**Smluvní strany**“ a jednotlivě jako „**Smluvní strana**“)

1. PŘEDMĚT SMLOUVY

1.1. Poskytovatel se zavazuje poskytovat Objednateli po dobu účinnosti této Smlouvy služby servisní podpory produktu AMIS*PACS FlexServer a dalších vybraných produktů dle čl. 2 této Smlouvy s tím, že Objednatel se za takto poskytnuté služby zavazuje hradit Poskytovateli měsíční odměnu.

2. ROZSAH POSKYTOVANÝCH SLUŽEB

2.1. Specifikace produktů, který je předmětem poskytovaných služeb:

- softwarový produkt **AMIS*PACS DicomRouter (ePACS)**
- softwarový produkt **AMIS*PACS FlexServer s licencí do 15TB,** vč. modulů:
- **Modul Integrace**
- **Modul Replikace**
- **Modul Komprese**
- **Modul Prefetching**
- **Modul Routing**
- softwarový produkt **ICZ*AZD s licencí na laboratorní výsledky**
- softwarový produkt **MedDream DICOM Viewer ve verzi LITE - 100 ks**
- softwarový produkt **MedDream DICOM Viewer ve verzi PRO - 8 ks**

- (dále „**Produkty**“)

2.2. Poskytovatel se zavazuje pro Objednatele poskytovat následující služby:

i. upgrade Produktů po dobu účinnosti Smlouvy, včetně instalace, v případě, kdy bude takový upgrade plošně Poskytovatelem poskytován,

ii. vzdálený nepřetržitý dohled Produktů,

iii. odstranění Chyb, Poruch nebo Havárií Produktů,

iv. poskytování podpory při konfiguraci systému – připojení nových modalit,

v. konfigurace front MWL,

vi. automatická offsite záloha dat po migraci na nové servery,

vii. pravidelná kontrola a údržba serveru,

viii. bezpečnostní aktualizace operačního systému

(dále vše společně jako „**Služby“**)

2.3. Výklad pojmů:

„Chybou“ se rozumí stav, kdy Produkty neplní některou z deklarovaných funkcí dle příslušné dokumentace.

„Poruchou“ se rozumí stav, kdy v Produktech nefunguje některá ze součástí, ale Produkt jako celek je funkční.

„Havárií“ se rozumí stav, kdy jsou Produkty jako celek nefunkční, především pak stav, kdy se neukládají data nebo data nejsou všeobecně dostupná.

2.4. Způsob a podmínky podání žádosti o provedení Služeb:

Požadavky na provedení Služeb budou předávány Poskytovateli výlučně prostřednictvím služby HelpDesk ICZ některým z těchto způsobů:

i. telefonicky na 222 272 222, 800 148 429 nebo 724 429 767

ii. přes www formulář na https://sdweb.i.cz/; přístup k tomuto formuláři mají pouze oprávněné osoby Objednatele na základě platných přístupových práv.

Z důvodu zajištění ochrany dat uložených v systému se Objednatel a Poskytovatel dohodli, že požadavky na provedení služeb jsou oprávněny za Objednatele předávat Poskytovateli pouze následující osoby:

jméno a příjmení	funkce	email	telefon
[redacted]			

Jakoukoli změnu osoby oprávněné předávat požadavky na provedení služeb stanovené v článku 2.4 je Objednatel povinen bezodkladně písemně oznámit Poskytovateli. Poskytovatel neodpovídá za vzniklou újmu v případě, kdy Objednatel Poskytovateli bezodkladně písemně neoznámí změnu osoby oprávněné předávat požadavky na provedení služeb.

2.5. Doba odezvy:

i. Začátek řešení Havárie bude v době od 7:00 do 16:00 hodin neprodleně, mimo pracovní dobu max. do 4 hodin od nahlášení Havárie.

ii. Začátek řešení Poruchy je max. do 6 hodin od nahlášení poruchy.

2.6. Povinnost Poskytovatele:

i. Poskytovatel je při provádění Služeb povinen dbát maximální opatrnosti a pečlivosti a postupovat tak, aby při provádění Služeb nedošlo k poškození, zničení, ztrátě nebo zneužití spravovaných dat, souborů dat a databází Objednatele.

ii. Poskytovatel je povinen zachovat mlčenlivost o skutečnostech a informacích získaných při manipulaci s daty Objednatele, zejména osobní data pacientů a údaje o jejich zdravotním stavu (dále „**citlivé osobní údaje**"). Poskytovatel je povinen chránit a utajovat citlivé osobní údaje před nepovolanými osobami.

iii. Poskytovatel neodpovídá Objednateli v rámci plnění dle této Smlouvy za chod a případná selhání systémů hardware po skončení záruky, sítí a systému zálohování.

iv. Poskytovatel je povinen dodržovat Pravidla chování poskytovatelů v oblasti bezpečnosti informací, která tvoří Přílohu č. 2 této Smlouvy

2.7. Povinnosti Objednatele:

i. Objednatel je povinen zajistit Poskytovateli jako nezbytný předpoklad provádění sjednaných Služeb konektivitu z vnitřní sítě Poskytovatele na servery, kterých se Služby dotýkají, a pokud to bude Poskytovatelem požadováno, i fyzický přístup k serverům, kterých se Služby dotýkají.

ii. Objednatel zajistí možnost vzdáleného dohledu Poskytovatele na funkčnost Produktu.

iii. Objednatel je povinen umožnit Poskytovateli přístup jako uživatel root na servery, kterých se poskytování Služeb dotýká.

iv. Objednatel je povinen oznámit a konzultovat s Poskytovatelem plánované změny v IT včetně síťové infrastruktury 24 hodin před provedením těchto změn.

v. Objednatel není oprávněn umožnit jakýkoli zásah do Produktu jakýmkoli třetím osobám včetně zaměstnanců a ostatních zástupců Objednatele bez předchozího souhlasu Poskytovatele.

vi. Objednatel je povinen zajistit bezproblémový chod, sítí a systému zálohování.

vii. Objednatel umožní přístup pověřeným pracovníkům Poskytovatele do prostor, ve kterých se provozuje zařízení s Produktem a případně i do dalších prostor, které s provozem zařízení souvisí, umožní pracovníkům Poskytovatele přístup do vnitřní sítě za účelem kontroly a testování funkčnosti Produktu. Tuto povinnost musí zajistit tak, aby nebránil Poskytovateli ve splnění lhůt definovaných v článku „Doba odezvy". V opačném případě se o dobu, po kterou neměli pracovníci Poskytovatele přístup k zařízení, prodlužují lhůty definované v článku „Doba odezvy".

3. MÍSTO A DOBA PLNĚNÍ

3.1. Místem plnění je sídlo Objednatele. Tam kde to je možné, provedení Služeb bude realizováno vzdáleným přístupem.

3.2. Smluvní strany konstatují, že Poskytovatel zahájil poskytování Služeb již **od dne 1. 7. 2023,** s výjimkou Služeb, vztahujícím se k produktům MedDream DICOM Viewer, jejichž poskytování Poskytovatel zahájí ke dni **1. 9. 2023.**

4. CENA POSKYTOVANÝCH SLUŽEB A PLATEBNÍ PODMÍNKY

4.1. Smluvní strany dohodly na paušální ceně za Služby ve výši **41 619,25 Kč měsíčně bez DPH** (dále „**Cena**"). S ohledem na dobu zahájení poskytování Služeb k produktům MedDream DICOM Viewer činí cena za poskytované Služby za měsíce červenec a srpen 2023 32 452,58 Kč bez DPH za každý z uvedených měsíců.

4.2. Cena náleží Poskytovateli bez ohledu na rozsah skutečně poskytnutých Služeb v daném kalendářním období (kalendářním období se rozumí období 1 měsíce) (dále „dílčí plnění") a je splatná dle pravidel uvedených v čl. 4.4 této Smlouvy.

4.3. Celková cena za poskytnuté Služby bude zvýšena o daň z přidané hodnoty (DPH). Daň z přidané hodnoty bude účtována v souladu se zák. č. 235/2004 Sb., v platném znění ke dni uskutečnění zdanitelného plnění, kterým je vždy poslední den daného měsíce, ve kterém byla služba poskytnuta. Objednatel se zavazuje uhradit celkovou cenu za poskytnuté služby na základě daňového dokladu, který bude vystaven do 15 dnů ode dne poskytnutí služby a má všechny náležitosti dle obchodních zvyklostí a zákonných předpisů platných pro vystavování daňových dokladů.

4.4. Cena je splatná na základě daňového dokladu – faktury vystavené vždy k poslednímu dni kalendářního měsíce, ve kterém byla služba poskytnuta. Faktura za první měsíc poskytování Služby bude, s ohledem na datum uzavření této Smlouvy, vystavena společně s fakturou za následující kalendářní období. Faktura je splatná 30 dní po jejím vystavení. Peněžité plnění se považuje za splněné okamžikem připsání částky na účet Poskytovatele. Všechny poplatky spojené s převodem peněz jdou k tíži plátce. Platba bude uskutečněna v Kč. V případě ukončení Smlouvy, má Objednatel právo požadovat zpět poměrnou část již uhrazené Ceny.

4.5. Námitky proti údajům uvedeným v daňovém dokladu může Objednatel uplatnit do 5 pracovních dnů ode dne obdržení faktury s tím, že ji prokazatelně odešle Poskytovatel i s uvedením výhrad. Pokud budou výhrady uznány jako oprávněné, tak nová lhůta splatnosti běží od okamžiku doručení opraveného daňového dokladu. Nedodržením lhůty pro vrácení faktury nebo neoprávněným vrácením faktury se doba splatnosti faktury nepřerušuje.

4.6. V případě prodlení Objednatele s peněžitým plněním je Poskytovatel oprávněn požadovat po Objednateli úrok z prodlení ve výši 0.05% z dlužné částky za každý započatý den prodlení.

5. VZÁJEMNÝ STYK SMLUVNÍCH STRAN

5.1. Osoby oprávněné jednat ve věci této Smlouvy jsou statutární orgány Smluvních stran nebo osoby, které k jednání a podepisování byly těmito orgány zplnomocněny nebo pověřeny.

5.2. Změna osob uvedených v odst. 5.1 musí být druhé straně oznámena bez zbytečného odkladu.

6. OCHRANA DŮVĚRNÝCH INFORMACÍ

6.1. Smluvní strany se zavazují, že budou chránit a utajovat před nepovolanými osobami důvěrné informace, informace získané při manipulaci s daty objednatele, zejména osobními daty pacientů a údaje o jejich zdravotním stavu podle zákona č. 372/2011 Sb., o zdravotních službách, Nařízení Rady (EU) č. 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů) a zákona č. 110/2019 Sb., o zpracování osobních údajů a skutečnosti tvořící obchodní tajemství (dále jen „**chráněné informace**“).

6.2. Poskytovatel se zavazuje, že chráněné údaje bude udržovat v tajnosti. Poskytovatel se zavazuje chráněné informace nesdělit třetí osobě, nezveřejnit ani nevyužít, ani neumožnit jejich využití třetí osobou. Poskytovatel nesmí chráněné informace jakkoli kopírovat nebo jinak rozmnožovat.

6.3. Smluvní strany se výslovně zavazují v rámci plnění této Smlouvy zajistit opatření k ochraně důvěrných informací Objednatele před jejich poškozením, ztrátou nebo zcizením a před neautorizovaným přístupem k těmto důvěrným informacím.

6.4. Poskytovatel nahradí Objednateli veškeré újmy (tj. škodu i nemajetkovou újmu), které Objednatel utrpí v důsledku porušení závazku mlčenlivosti a ochrany důvěrných informací. Závazek k ochraně a utajení trvá po celou dobu existence chráněných důvěrných informací.

7. UKONČENÍ SMLOUVY

7.1. Kterákoli ze smluvních stran je oprávněna vypovědět Smlouvu písemně, a to i bez udání důvodu s výpovědní dobou tří (3) měsíců, jež počíná běžet prvního dne měsíce následujícího po měsíci, ve kterém byla výpověď doručena.

7.2. Smlouvu je možné ukončit písemnou dohodou Smluvních stran, jejíž součástí je i vypořádání vzájemných závazků a pohledávek.

7.3. Smluvní strana je dále oprávněna odstoupit od Smlouvy mj. v případě, že druhá smluvní strana přes písemné upozornění na podstatné porušení smlouvy toto porušení v poskytnuté lhůtě, která nesmí být kratší než 15 dnů, neodstranila.

8. ZÁVĚREČNÁ USTANOVENÍ

8.1. Smlouva nabývá platnosti dnem jejího podpisu oběma Smluvními stranami a uzavírá se na dobu jednoho roku od zahájení poskytování Služeb. Smluvní strany se dohodly, že vybraná ustanovení této Smlouvy, resp. odst. 1.5, 1.6 a 7.4 Přílohy č. 2 této Smlouvy, která se vztahují k penetračním testům, analýze rizik a dokumentaci, budou aplikovatelná počínaje 1.1.2024, a to s ohledem na jejich postupné zavádění Poskytovatelem.

8.2. V případě, že Smlouva podléhá zveřejnění v registru smluv ve smyslu zákona č. 340/2015 Sb., zákon o registru smluv, tak nabývá účinnosti dnem jejího zveřejnění v registru smluv s tím, že Smluvní strany se dohodly, že zveřejnění Smlouvy zajistí Objednatel.

8.3. Tato Smlouva se řídí právním řádem České republiky.

8.4. Veškeré změny či doplnění Smlouvy lze činit pouze na základě písemné dohody smluvních stran. Takové dohody musí mít podobu datovaných, číslovaných a oběma smluvními stranami podepsaných dodatků Smlouvy.

8.5. Všechna vyhotovení Smlouvy jsou rovnocenná a mají platnost originálu.

8.6. Tato Smlouva je vyhotovena ve dvou shodných výtiscích, z nichž Objednatel i Poskytovatel obdrží jedno vyhotovení.

8.7. Nedílnou součástí této Smlouvy jsou také následující přílohy:

Příloha č. 1 - Plná moc od ICZ a.s. [redacted]
Příloha č. 2 - Pravidla chování poskytovatelů v oblasti bezpečnosti informací

V Písku dne _____

Za Nemocnici Písek, a.s.:

_____
MUDr. Jiří Holan, MBA
předseda představenstva

V Praze dne _____

Za ICZ a.s.:

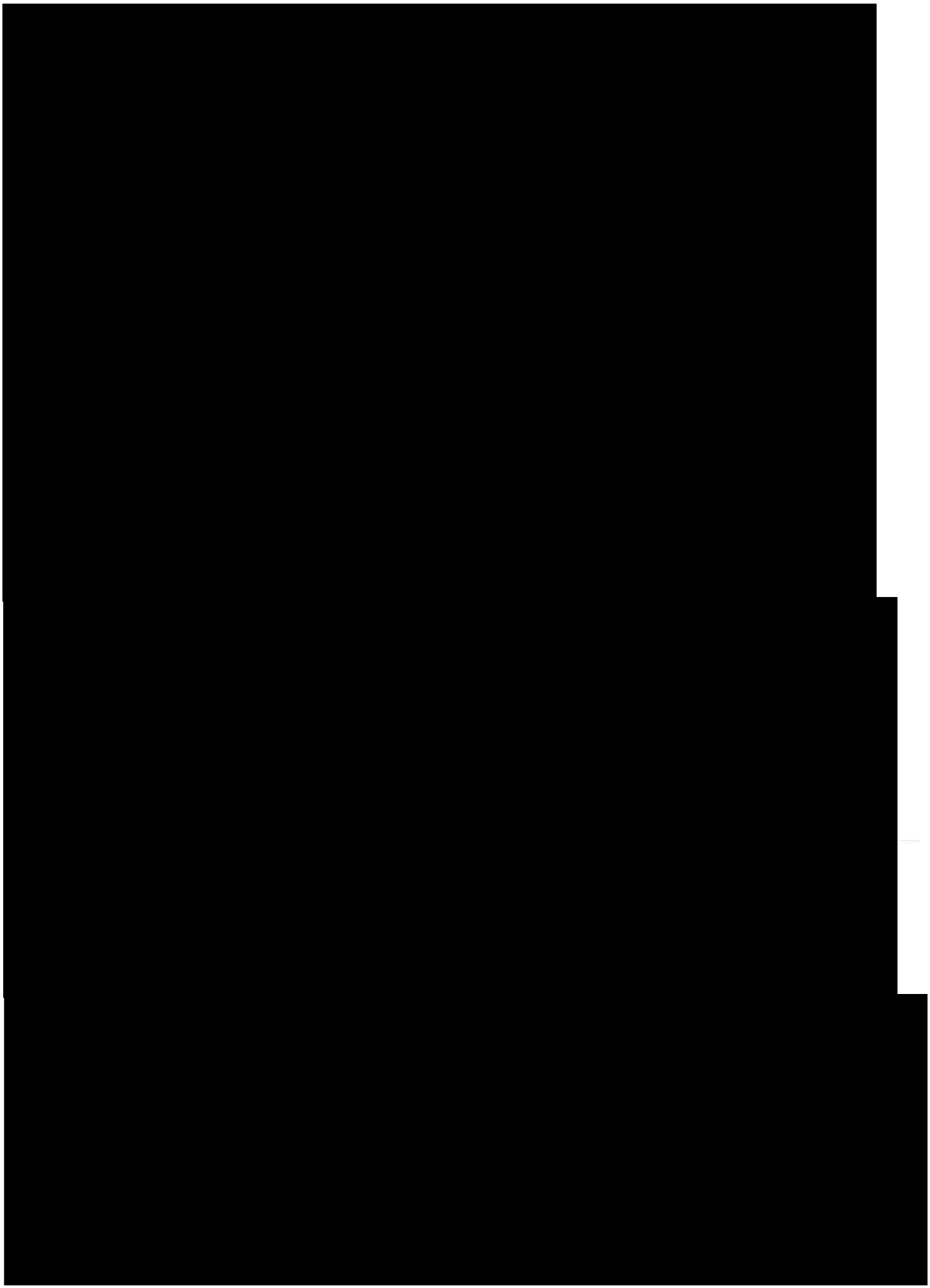
_____
[redacted]

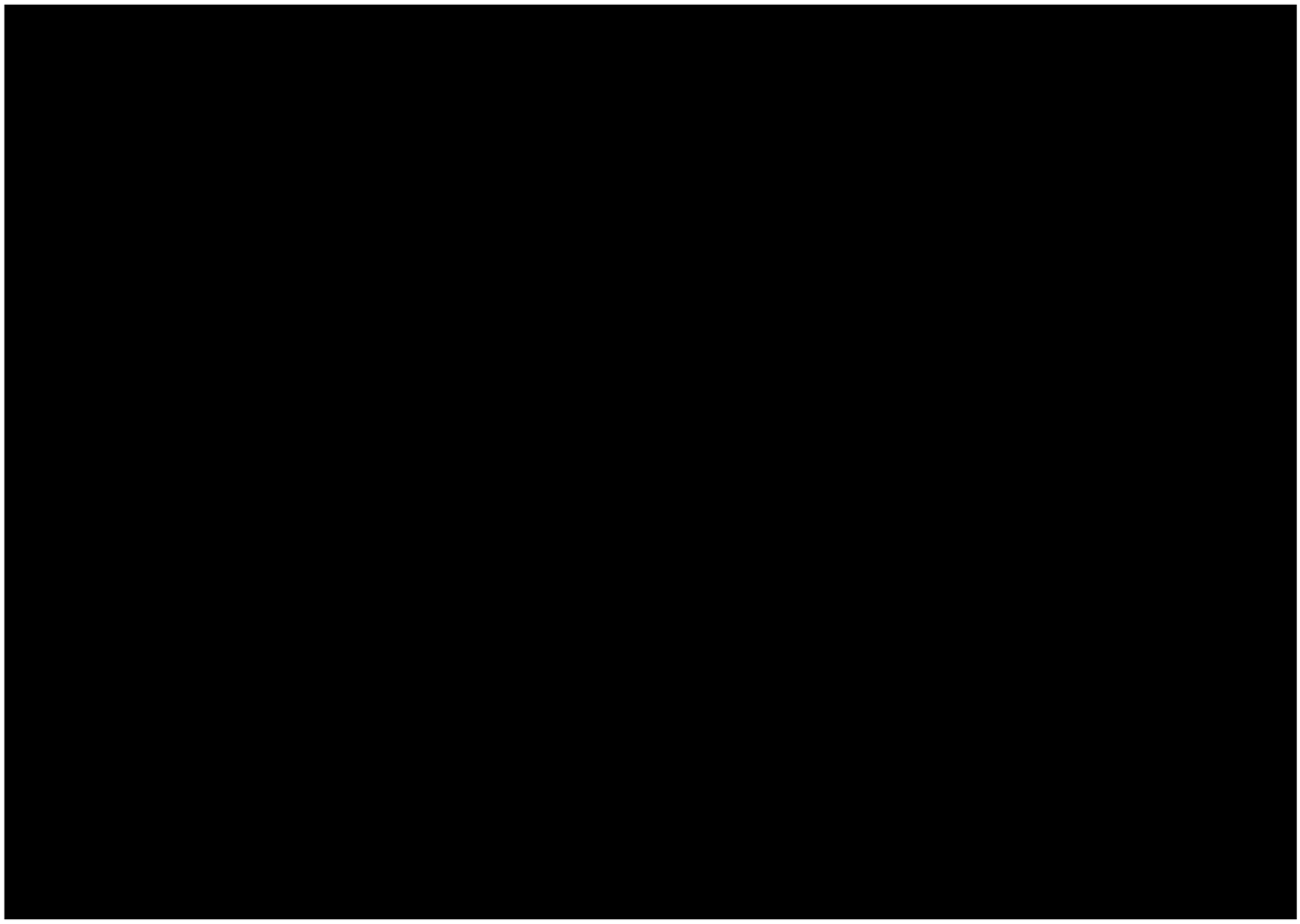
_____
Ing. Dana Čagánková
člen představenstva

Příloha č 1

Plná moc od ICZ a.s. pro [redacted]

PLNÁ MOC





Příloha č 2

Pravidla chování poskytovatele v oblasti bezpečnosti informací

1. Obecná pravidla

   1.1. Předmět plnění dle Smlouvy o poskytování služeb (dále Předmět plnění) nesmí být zatížen žádnými faktickými ani právními vadami a musí odpovídat všem technickým požadavkům, technickým a bezpečnostním normám pro daný druh Předmětu plnění.

   1.2. Zaměstnanci Poskytovatele mohou přistupovat k informačním a komunikačním prostředkům (ICT prostředky) Objednatele výhradně prostřednictvím uživatelských účtů, které jim byly přiděleny Objednatelem.

   1.3. Poskytovatel se zavazuje nakládat s veškerými daty, informacemi a údaji, ke kterým se dostane v rámci Předmětu plnění takovým způsobem, aby nemohlo dojít k jejich ztrátě, vyzrazení, neoprávněné či neodborné manipulaci. Dále se zavazuje používat tato data pouze k danému účelu a neumožnit jejich zpřístupnění nepovolané osobě.

   1.4. Poskytovatel se zavazuje dodržovat veškerou platnou legislativu, zejména pak tu v oblasti kybernetické bezpečnosti a ochrany osobních údajů.

   1.5. Poskytovatel musí mít ustanoven a dodržovat Systém Řízení Bezpečnosti Informací (ISMS). Na vyžádání Objednatele je Poskytovatel povinen předložit analýzu rizik, která se týká Předmětu plnění.

   1.6. Poskytovatel je povinen zajistit odpovídající kvalitu Předmětu plnění. K prokázání úrovně bezpečnosti může Poskytovatel poskytnout report výsledků penetračního testu Předmětu plnění. Z důvodu objektivity je nutné, aby tyto testy nebyly prováděny interně Poskytovatelem, ale musí být realizovány nezávislou firmou. Penetrační testy jsou realizovány minimálně pro každý „major release“ Předmětu plnění. Poskytovatel je povinen na vyžádání poskytnout závěrečnou zprávu těchto penetračních testů, ve které jsou jednotlivé zranitelnosti ohodnoceny pomocí CVSS v3.1. Předmět plnění nesmí obsahovat žádné zranitelnosti ohodnocené jako High či Critical (7.0-10.0). Zranitelnosti, které byly ohodnoceny jako Medium (4.0-6.9) musí písemně akceptovat manažer kybernetické bezpečnosti Objednatele. Pokud nebude tento report dodán, dojde ke zneužití zranitelnosti Předmětu plnění, který bude mít dopad na běžný provoz Objednatele, pak za způsobenou škodu odpovídá Poskytovatel.

   1.7. Poskytovatel je povinen umožnit Objednateli provedení auditu kybernetické bezpečnosti předmětu plnění. Objednatel si může najmout externí konzultační firmu, která tento audit provede. Předmětem auditu bude zejména plnění pravidel, ke kterým se Poskytovatel smluvně zavázal. Audit je možné provádět po předchozí domluvě jednou za dva roky či v případě důvodného podezření na porušení plnění smluvních závazků ze strany Poskytovatele.

   1.8. Veškerá ustanovení těchto pravidel musí být promítnuta i k jednotlivým subdodavatelům Poskytovatele. Za plnění subdodavatele odpovídá vůči Objednateli Poskytovatel.

2. Uživatelská oprávnění

   2.1. Poskytovatel poskytne Objednateli seznam uživatelů, kteří potřebují přistupovat k ICT prostředkům Objednatele. Každému uživateli bude vytvořen vlastní uživatelský účet s minimální sadou oprávnění, kterou potřebuje ke své činnosti. Přidělená oprávnění podléhají schválení manažerem kybernetické bezpečnosti Objednatele. O schválení je nutné uchovávat písemný záznam.

   2.2. Sada oprávnění jednotlivých uživatelů a jejich aktuálnost je pravidelně (minimálně jednou ročně) validována manažerem kybernetické bezpečnosti Objednatele. Poskytovatel je povinen poskytnout k této validaci součinnost. O proběhlé kontrole je uchováván písemný záznam.

   2.3. Přidělené účty není povoleno sdílet mezi různými zaměstnanci Poskytovatele. V takovém případě se jedná o podstatné porušení Smlouvy o poskytování služeb a těchto pravidel.

3. Ustanovení o oprávnění užívat data

3.1. Veškerá data získaná, zpracovaná a uložená v rámci Předmětu plnění (dále Data) jsou ve výhradním vlastnictví Objednatele. Poskytovatel má k těmto datům primárně užívací právo.

3.2. Poskytovatel se zavazuje zachovávat důvěrnost, dostupnost i integritu uložených Dat. K Datům mohou přistupovat pouze autorizovaní a proškolení zaměstnanci Poskytovatele. Poskytovatel je povinen veškeré přístupy k Datům evidovat.

3.3. V případě ukončení spolupráce je Poskytovatel povinen Data předat Správě ICT. Data musí být předána v otevřeném a strojově čitelném formátu do deseti dnů od ukončení platnosti smlouvy. O tomto předání bude vyhotoven písemný protokol.

4. Bezpečnost komunikace

4.1. V případě ztráty nebo odcizení hardware, software, dat, informací ve vlastnictví Objednatele musí Poskytovatel vždy neprodleně nahlásit tuto skutečnost Objednateli. Nahlášení provede vždy na e-mail: security@nemopisek.cz a telefonicky na tel.: +420 382 772 001. (Objednatel výslovně vyžaduje duplicitní informaci, tedy telefonem a zároveň i e-mailem).

4.2. Při práci na zařízení (například: počítači, notebooku, mobilním telefonu, zdravotnickém prostředku) připojeném do sítě a/nebo k informačním systémům Objednatele musí Poskytovatel dodržovat tyto zásady:

- k zařízení může přistupovat pouze autorizovaný zaměstnanec Poskytovatele, který byl Poskytovatelem prokazatelně proškolen ohledně kybernetické bezpečnosti,
- chránit výpočetní techniku a všechna data Objednatele před porušením důvěrnosti, integrity či dostupnosti,
- po ukončení práce v síti a/nebo v informačním systému Objednatele provést neprodleně odhlášení uživatele.

4.3. Při práci na serverech Objednatele musí být splněny následující zásady:

- server svěřený Poskytovateli do správy musí Poskytovatel pravidelně udržovat a kontrolovat zejména z pohledu bezpečnosti, dostupnosti a integrity dat,
- nesmí měnit jakákoliv oprávnění na serveru nebo informačním a komunikačním systému bez písemného souhlasu odboru Správy sítě a výpočetní techniky Nemocnice Písek, a.s. (dále jen „Správa ICT“,
- Poskytovatel nesmí měnit nastavení operačního systému serverů a jeho komponent bez souhlasu odboru Správy ICT,
- Poskytovatel musí zajistit bezpečnostní aktualizaci operačního systému a aplikačních částí serverů; bezpečnostní aktualizace kritického charakteru, které mohou ohrozit bezpečnost sítě Objednatele musí aplikovat neprodleně po jejich vydání,
- Poskytovatel je povinen udržovat aktuální dokumentaci k provozovaným informačních a komunikačním systémům, kterou po každé aktualizaci musí předat Správě ICT,

4.4. Při práci v interní sítí Objednatele odpovídají zaměstnanci Poskytovatele, kteří mají přidělen přístup do interní sítě Objednatele, za své činnosti prováděné v rámci této sítě. Zaměstnanci Poskytovatele nesmí, zejména:

- zneužívat síťové prostředky pro osobní účely a zatěžovat kapacitu sítě,
- šířit či jinak nakládat se škodlivým malwarem,
- využívat nástroje sloužící k maskování identity,
- provádět bezdůvodné skenování portů či jiných parametrů sítě a síťových zařízení. V případě nutnosti, musí být spuštění těchto skenů schváleno písemně manažerem kybernetické bezpečností Objednatele,

- provádět jakoukoliv formou monitorování sítě, které může vést k zachycení dat, pokud to není Předmětem plnění smlouvy s Objednatelem,
- obcházet autentizaci uživatele nebo obcházet zabezpečení jakéhokoliv počítače, sítě nebo uživatelského účtu,
- provádět jakékoliv nepracovní aktivity. Zejména pak ty, které mohou vést k omezování nebo odepírání služeb jiným uživatelům,
- užívat jakékoliv programy, skripty nebo příkazy, které mohou znamenat ohrožení kyberbezpečnosti Objednatele. Například spuštění skriptu získaného z veřejného repositáře (např. z GitHubu) je možné pouze na vlastní odpovědnost zaměstnance Poskytovatele,
- užívat jakékoliv programy, skripty nebo příkazy, nebo zasílat zprávy v jakékoliv formě s úmyslem omezit nebo znemožnit poskytování služeb nebo terminálových relací lokálně nebo přes síť, internet nebo intranet,
- využívat bezpečnostních mezer nebo vytvářet útoky na komunikaci v počítačových sítích
- předávat informace o konfiguraci a topologii sítě cizím osobám (i v rámci společnosti Poskytovatele); tyto informace je oprávněn předat pouze odpovědný zaměstnanec Objednatele, pokud jsou takové informace nutné z hlediska přípravy či Předmětu plnění.

5. Kybernetické bezpečnostní události a incidenty

5.1. Poskytovatel musí vyvinout maximální úsilí pro odvracení bezpečnostních hrozeb a kybernetických útoků pro informační a komunikační systémy Objednatele.

5.2. Poskytovatel musí zajistit maximální součinnost při analýze kybernetických bezpečnostních událostí a incidentů Objednatele a následně zavádět vhodná nápravná opatření určené Objednateli.

5.3. V případě vážného podezření či potvrzení vzniku bezpečnostní hrozby pro informační a komunikační systém NP je Poskytovatel povinen neprodleně písemně informovat o této skutečnosti Manažera kybernetické bezpečnosti na e-mail: security@nemopisek.cz a telefonicky na tel.: +420 382 772 001. (Objednatel výslovně vyžaduje duplicitní informaci, tedy telefonem a zároveň i e-mailem).

6. Požadavky na dodávané informační systémy

6.1. Informační systém musí být vytvářen tak, aby dostatečně chránil data před porušením důvěrnosti, dostupnosti a integrity.

6.2. Informační systém musí být vytvořen tak, aby byla každá operace uložena v provozním záznamu (logu) s jedinečným identifikátorem uživatele, který tuto operaci vykonal. Musí být zajištěno, aby nemohlo dojít k provádění operací pod cizím identifikátorem uživatele. Aplikace nemůže modifikovat či mazat dříve uložené záznamy, pouze přidávat nové.

6.3. Uživatel informačního systému musí být nucen si heslo pravidelně měnit. Hesla musí splňovat minimálně aktuální bezpečnostní nároky, které stanovil NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost).

6.4. Informační systém musí být vytvořen tak, aby byl počet neúspěšných pokusů o přihlášení omezen. Po pěti neúspěšných pokusech o přihlášení musí být další zadávání dočasně zablokováno nebo spojení rozpojeno.

6.5. V případě, že je povolen přístup do informačního systému, v němž určuje vstupní heslo administrátor, je povinností autora informačního systému vynutit si změnu tohoto inicializačního hesla.

6.6. Poskytovatel nesmí používat jedno přihlašovací jméno pro několik svých zaměstnanců, každý účet musí být jmenný.

6.7. V informačních systémech musí být pořizovány auditní záznamy obsahující alespoň:

- identifikaci uživatele;
- datum a čas přihlášení a odhlášení;
- identifikaci místa, odkud se uživatel přihlašoval (pokud je to možné);
- záznamy o přístupu (úspěšném i neúspěšném), případně o prováděných operacích;
- záznamy musí být možné vzdáleně číst a následně zpracovávat.

6.8. Řízení přístupu k informačním systémům

- Před umožněním přístupu musí být každý uživatel identifikován a autentizován.
- Informační systém by měl po určité době nečinnosti uživatele (doporučeno 15 minut) tohoto uživatele odhlásit.
- Po určitém množství neúspěšných autentizačních pokusů (doporučeno 5) se musí ukončit přihlašovací proces.
- V případě neúspěšné autentizace nesmí informační systém poskytnout uživateli informaci o tom, která část autentizace je chybná.
- Pro každého uživatele informačního systému musí být možné identifikovat, jaká má přístupová práva.
- Pro každý prostředek musí být možné vytvořit seznam uživatelů, kteří mají přístupová práva k tomuto prostředku s rozlišením druhu přístupových práv (čtení, úprava atd.).
- Informační systém musí mít mechanismus pro odejmutí všech přístupových práv konkrétnímu uživateli nebo skupině.

6.9. Data vstupující do informačních systémů musí být kontrolována tak, aby byla zajištěna jejich správnost. V informačních systémech se musí evidovat identifikátor uživatele, který změny provedl. Pro kontrolu dat musí Poskytovatel aplikovat zejména tato opatření:

- vstupní kontrola (neplatné znaky, rozsah, přetečení, kompletnost, souvislost...),
- kontrola vnitřního zpracování dat,
- kontrola oprávněnosti běhu programů,
- kontrola integrity dat,
- kontrola obsahu generovaných dat.

6.10. Vývoj software musí probíhat:

- legálním softwarem,
- autorská a licenční ujednání musí být smluvně řešena před samotným vývojem,
- na testovacím prostředí odděleném od prostředí produkčního,
- na testovacích datech, která nejsou převzata z provozní databáze; pokud je nutné použít data z provozní databáze, je nutné je anonymizovat,
- migrace do provozního prostředí může být provedena až po akceptaci výsledků testů ve vývojovém či testovacím prostředí.

7. Předání plnění

Je-li informační systém vyvíjen na zakázku, musí splňovat všechny níže uvedené body a jedná-li se o již vyvinutý informační systém, musí být tyto požadavky zohledněny v hlavní smlouvě.

7.1. Dodávka software

- U veškerého dodávaného programového vybavení musí být zřejmé, zda se jedná o volně šířený software nebo program podléhající licenční a registrační politice. Pracuje-li počítačový program nebo aplikace, s daty, musí být specifikováno s jakými daty a musí být provedena jejich kategorizace.

7.2. Dodávka hardware

- Ke každé dodávce musí existovat kromě účetních dokladů i předávací protokol podepsaný Poskytovatelem a Objednatelem. Způsob předání závisí na konkrétním hardware a na smlouvě s Poskytovatelem.

7.3. Dodávka služeb

- Způsob předání závisí na konkrétní službě a na smluvních podmínkách dohodnutých ve Smlouvě.

7.4. Dokumentace

- Nedílnou součástí dodávky Předmětu plnění je projektová a bezpečnostní dokumentace Předmětu plnění. Rozsah a náplň dokumentace musí být specifikován ve smlouvě s Poskytovatelem. Chybějící, neúplná nebo neaktuální dokumentace je důvodem k reklamaci dodávky a v případě, že ji Poskytovatel ve lhůtě stanovené Objednatelem neopraví, důvodem k odstoupení od Smlouvy.

7.5. Akceptace

- Každý dodávaný prvek Předmětu plnění musí být plně a široce Poskytovatelem otestován, zda splňuje očekávané a smluvně definované parametry, a zda jeho používání nepředstavuje neočekávaná bezpečnostní rizika (penetrační test, práce s daty).
- Každý prvek Předmětu plnění je předán až podpisem písemného předávacího protokolu oprávněnými zástupci smluvních stran.

8. Fyzická bezpečnost

8.1. Na neveřejných pracovištích a prostorách Objednatele (např. serverovny, sklady) není dovolen pohyb nepovolaných osob bez dozoru zaměstnance Objednatele.

8.2. Zaměstnanci Poskytovatele mohou fyzicky přistupovat k ICT prostředkům Objednatele pouze v doprovodu oprávněné osoby Objednatele.

8.3. V případě práce Poskytovatele v prostorách Objednatele nebo v jím využívaných prostorách v datových centrech musí Poskytovatel dále dodržovat tyto zásady:

- připojovat vlastní počítač, notebook pouze se souhlasem odpovědné osoby Objednatele,
- v blízkosti ICT prostředků nejíst, nepít a nekouřit.

8.4. Poskytovatel není oprávněn k výměně a odvozu použitých či vadných technologií bez písemného souhlasu Správy ICT. A to ani v případě zařízení spravovaných Poskytovatelem.

8.5. V případě poškození či výměny (povolené Správou ICT) některého z nosičů dat, na kterém byly uloženy Data pacientů, je nutné zajistit bezpečnou likvidaci hmotného nosiče dat. Tato likvidace musí být řádně zaprotokolována.

9. Porušení pravidel

9.1. Porušení těchto pravidel představuje porušení Předmětu plnění. Pokud Poskytovatel poruší tato pravidla hrubým způsobem nebo opakovaně, je Objednatel oprávněna odstoupit od smluvního vztahu s Poskytovatelem.