Smlouva o poskytování servisních služeb č. 812/22/13/SIS

Článek 1
Smluvní strany

Fakultní nemocnice Plzeň
sídlo: Edvarda Beneše 1128/13, 305 99 Plzeň
IČ: 00669806
DIČ: CZ669806
zastoupená: MUDr. Václavem Šimánkem, Ph.D., ředitelem
bankovní spojení: Česká národní banka, č. ú. 33739311/0710
datová schránka: pbvtj63
(dále jen „Objednatel“)

a

GEM System a.s.
se sídlem: Na Pankráci 1062/58, 140 00 Praha 4
IČ: 27189929
DIČ: CZ 27189929
zastoupená: Ing. Michal Pajr – Místopředseda představenstva
bankovní spojení: Česká spořitelna, a.s. číslo účtu: 176510389/0800
datová schránka: hp47z64
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 17281
(dále jen „Poskytovatel“)

uzavírají tuto Smlouvu o poskytování servisních služeb (dále také jen „Smlouva“) podle § 1746 a násl. zákona č. 89/2012 Sb., občanského zákoníku, v platném znění (dále jen „občanský zákoník“)

Článek 2
Předmět Smlouvy

1. Předmětem Smlouvy je poskytování podpory provozu databázového prostředí Oracle Enterprise Edition (dále jen Oracle EE) a Oracle Standard Edition 2 (dále jen Oracle SE2) a operačního systému (dále jen OS) RedHat, na němž je provozováno, a nepřetržitý monitoring celého prostředí v rozsahu definovaném ve Smlouvě, vše po dobu 2,5 roku.
2. Poskytovatel podpisem Smlouvy garantuje Objednateli splnění všech podmínek obsažených v zadávací dokumentaci veřejné zakázky uvedené v odst. 1.

Článek 3
Definice rozsahu služeb

3. Podpora bude zahrnovat následující části:
   a) Podpora provozu
   b) Nepřetržitý monitoring

Detailní popis součástí podpory je uveden v příloze č. 1 Smlouvy.

Článek 4
Místo a způsob plnění

1. Služby mohou být poskytovány pomocí vzdáleného přístupu do sítě Objednatele, v případě nutnosti i v provozovně Objednatele.
2. Pokud bude Poskytovatel využívat vzdálený přístup, sjednávají smluvní strany, že bude realizován prostřednictvím zabezpečeného kanálu sítě Internet, k datu uzavření Smlouvy je sjednán způsob připojení prostřednictvím Forticlient VPN. Podmínky pro přístup Poskytovatele do vnitřní sítě FN Plzeň prostřednictvím VPN jsou uvedeny v příloze č. 5 Smlouvy. Objednatel je oprávněn jednostranně změnit řešení pro vzdálený přístup dle svých aktuálních standardů. O této skutečnosti je povinen informovat Poskytovatele pomocí e-mailu zaslaného nejméně 1 týden předem na adresu fnplzen@gemsupport.cz

Článek 5
Cena a platební podmínky

1. Cena předmětu Smlouvy je stanovena v celkové výši 1 680 000 Kč za období platnosti Smlouvy, tedy za 2,5 roku. Cena je uvedena bez DPH. Detailní rozpis ceny je uveden v příloze č. 3 Smlouvy.
2. Ceny jednotlivých položek jsou cenami nejvýše přípustnými po celou dobu plnění. To znamená, že v průběhu realizace zakázky nesmí být v žádném případě překročeny nebo jakkoliv navyšovány.
3. Cena zahrnuje veškeré náklady na splnění předmětu Smlouvy, včetně nákladů na dopravu, čas strávený na cestě a ubytování pracovníků pověřených Poskytovatelem k provádění díla.
4. Smluvní strany se dohodly, že servisní podpora bude fakturována měsíčně, vždy k poslednímu dni každého měsíce trvání Smlouvy. Částka k měsíční fakturaci je 56 000 Kč bez DPH. K této částce bude přičtena DPH v zákonné výši.
5. Faktury bude Poskytovatel zasílat elektronicky ve formátu PDF na e-mail: fakturace@fnplzen.cz a to nejpozději do 7. kalendářního dne ode dne uskutečnění zdanitelného plnění.
6. Splatnost faktury je smluvně stanovena na 30 kalendářních dnů od data vystavení.
7. Faktury musí obsahovat náležitosti daňového dokladu dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a také registrační číslo smlouvy Objednatele.
8. V případě, že účetní doklady nebudou mít odpovídající náležitosti nebo cena nebude odpovídat Smlouvě, je Objednatel oprávněn zaslat je ve lhůtě splatnosti zpět Poskytovateli k doplnění, aniž se tak dostane do prodlení se splatností; lhůta splatnosti počíná běžet znovu od opětovného zaslání náležitě doplněných či opravených dokladů.
9. Faktura se považuje za uhrazenou předáním neodvolatelného platebního příkazu ze strany Objednatele bance.

Článek 6
Práva a povinnosti Objednatele

1. Objednatel je povinen zaplatit Poskytovateli cenu ve výši a způsobem popsaným v čl. 5 Smlouvy.
2. Objednatel je povinen poskytnout Poskytovateli nezbytnou součinnost a veškeré potřebné informace, které jsou nezbytné pro řádné plnění předmětu této Smlouvy.

Článek 7
Práva a povinnosti Poskytovatele

1. Poskytovatel je povinen poskytovat Objednateli služby v rozsahu a v časových limitech pro poskytování těchto služeb stanovených Smlouvou.
2. Poskytovatel je povinen zajistit řádnou obsluhu a dostupnost HelpDeskového portálu pro hlášení nestandardních stavů a servisních požadavků i servisního telefonu HotLine pro hlášení nestandardních stavů nepřetržitě, 24 hodin, 7 dní v týdnu. 365 dní v roce.
3. Poskytovatel je povinen poskytnout Objednateli přístupová oprávnění na HelpDeskový portál pro zaměstnance, pro něž o to Objednatel požádá. Jejich seznam předá oprávněná osoba Objednatele ve věcech technických.
4. Poskytovatel je povinen zacházet s veškerými daty, s nimiž přijde v rámci své činnosti dle Smlouvy do styku, jako s důvěrnými a neposkytovat je třetím osobám, ani je jiným způsobem nevyužívat.

Článek 8
Oprávněné osoby a kontakty

1. Seznam oprávněných osob Objednatele i Poskytovatele, vč. oblastí působení a kontaktů jsou uvedeny v příloze č. 2 Smlouvy.
2. HelpDeskový portál je provozován na adrese https://www.gemsupport.cz

Článek 9
Ochrana informací

1. Smluvní strany tímto prohlašují, že berou na vědomí, že při plnění této smlouvy může dojít ke zpřístupnění informací, které jsou považovány za důvěrné a tyto informace mohou být zpřístupněny rovněž zaměstnancům druhé smluvní strany.
2. Smluvní strany se zavazují, že během platnosti této smlouvy nezpřístupní žádné třetí straně jakékoliv informace, které byly v souvislosti s plněním dle této smlouvy poskytnuty mezi smluvními stranami (ať již úmyslně nebo opomenutím) a mají důvěrný charakter. Tato povinnost se však nevztahuje na:
    a) informace, na jejichž zpřístupnění se smluvní strany dohodly;
    b) jakékoliv sdělení učiněné smluvním stranám, zástupcům nebo zaměstnancům, jejichž znalost takovýchto informací je nezbytná k řádnému plnění této smlouvy; a
    c) každou informaci, která byla dostupná veřejnosti se souhlasem strany, od níž pochází, nebo se stala veřejným majetkem jinak než porušením této smlouvy přijímající stranou;
    d) každou informaci získanou přijímající stranou od třetí strany bez povinnosti mlčenlivosti; a
    e) informace, které jsou smluvní strany povinny poskytovat na základě platných právních předpisů.

    Výše uvedené se nevztahuje na osobní údaje a údaje zvláštní kategorie pacientů a klientů objednatele, tyto údaje zůstávají důvěrnými za všech okolností. Jejich ochraně se věnuje článek 10 Smlouvy.

3. Pro účely Smlouvy se za důvěrné informace považují všechny informace, které jsou nebo mohou být součástí obchodního tajemství, zejména:
    a) popisy technologických postupů, procesů a vzorců nebo jejich části;
    b) technické vzorce;
    c) technické know-how;
    d) informace o provozních metodách, procedurách a pracovních postupech;
    e) obchodní nebo marketingové plány, koncepce a strategie nebo jejich části;
    f) nabídky, smlouvy, dohody a jiná ujednání se třetími stranami;
    g) informace o výsledcích hospodaření;
    h) informace o vztazích s obchodními partnery;
    i) informace o pracovněprávních otázkách;
    j) veškeré další informace, jejichž zveřejnění by mohlo smluvní straně způsobit škodu.
4. Jsou-li důvěrné informace poskytovány v písemné nebo elektronické podobě, je nezbytné toto na dokumentech označit alespoň na první straně každého dokumentu obsahujícího důvěrné informace. Tato povinnost se nevztahuje na osobní údaje a údaje zvláštní kategorie pacientů nebo klientů objednatele, ty jsou považovány za důvěrné vždy.
5. Smluvní strany se dohodly, že povinnost mlčenlivosti dle tohoto ustanovení Smlouvy přetrvá i po jejím skončení.

Článek 10
Ochrana osobních údajů a údajů zvláštní kategorie

1. Vzhledem ke skutečnosti, že v rámci smluvního vztahu založeného Smlouvou umožňuje v nezbytných případech objednatel Poskytovateli přístup k osobním údajům a údajům zvláštní kategorie subjektů údajů svých klientů a pacientů (dále jen „Klienti“), ve smyslu zákona č. 110/2019 Sb., o zpracování osobních údajů (dále jen „Zákon o zpracování osobních údajů“) a Nařízení Evropského parlamentu a Rady (EU) 2016/679 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 (dále jen „Nařízení“), zpřesňují Smluvní strany svá práva a povinnosti při zpracování osobních údajů a údajů zvláštní kategorie Klientů objednatele v souladu s uvedenými právními předpisy následovně.

2. Poskytovatel se zavazuje zachovávat mlčenlivost o všech skutečnostech, o nichž se dozví u objednatele při plnění závazků dle této smlouvy nebo v souvislosti s nimi. To platí zejména o skutečnostech, na něž se vztahuje povinnost mlčenlivosti zdravotnických pracovníků, zejména podle ustanovení § 51 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (Zákon o zdravotních službách), jakož i o osobních údajích a osobních údajích zvláštní kategorie (dále jen „Osobní údaje“) a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení Osobních údajů ve smyslu zejména ustanovení § 32 a § 47 Zákona o zpracování osobních údajů. Poskytovatel se zavazuje nakládat s Osobními údaji v souladu s Nařízením, Zákonem o zpracování osobních údajů a prováděcími právními předpisy přijatými k ochraně a zpracování Osobních údajů.
3. Pokud Poskytovatel přijde při plnění této smlouvy do styku s Osobním údajem a bude v postavení zpracovatele (dále jen „Zpracovatel“) ve smyslu Nařízení a Zákona o zpracování osobních údajů, zavazuje se nakládat s Osobními údaji pouze za účelem splnění závazků z této smlouvy a žádným jiným způsobem, a to v souladu s Nařízením a Zákonem o zpracování osobních údajů a Zákonem o zdravotních službách a prováděcími předpisy.
4. Osobní údaje nebudou použity k jinému účelu než k plnění této smlouvy, ani z nich nebudou odvozovány informace pro žádné reklamní či jiné komerční účely.
5. Poskytovatel bere na vědomí, že při plnění této smlouvy může přijít do styku s následujícími Osobními údaji Klientů – jméno, příjmení, titul, rodné číslo, resp. číslo pojištěnce nebo datum narození, číslo pojišťovny, anamnestická data související se zdravotním stavem a péčí o Klienta, diagnosy, adresa bydliště anebo pobytu, telefonní číslo, e-mailová adresa, identifikační údaje zaměstnavatele, profese, informace o rodinných příslušnících, pohlaví, rodinný stav, občanství, identifikační údaje praktických lékařů Klienta, druh a výše sociální dávky.
6. Jakékoliv nakládání s Osobními údaji je nutné považovat za zpracování Osobních údajů.
7. Za porušení ochrany Osobních údajů v průběhu plnění této smlouvy je odpovědný Poskytovatel.
8. Poskytovatel je oprávněn zpracovávat Osobní údaje pouze po dobu trvání závazku mezi smluvními stranami anebo po dobu nezbytnou k plnění archivačních povinností podle platných právních předpisů, nejdéle však 10 let od jejího ukončení.
9. Po ukončení této smlouvy se Poskytovatel zavazuje veškeré Osobní údaje, které má případně ve své k dispozici např. za účelem provádění testování anebo jiných operací za účelem zvýšení anebo ověření kvality systému prokazatelně smazat nebo vrátit objednateli a vymazat existující kopie, neukládá-li zákon Poskytovateli povinnost Osobní údaje zpracovávat i po ukončení této smlouvy.
10. Poskytovatel za účelem ochrany Osobních údajů objednatele a jeho Klientů před neoprávněným přístupem, použitím, zveřejněním nebo zničením, resp. před jejich náhodnou ztrátou či změnou uplatňuje technická a organizační bezpečnostní opatření, interní kontroly a rutiny zabezpečení Osobních údajů zajišťující splnění všech povinností dle Nařízení a Zákona o zpracování osobních údajů, zejména zajišťuje, aby veškeré přístupy byly možné pouze přes přístupová hesla pouze výslovně oprávněných pracovníků Poskytovatele, se záznamem historie o přístupu do IS objednatele, a dále aby data obsažená ve zdravotnické dokumentaci objednatele byla šifrována způsobem, který znemožní nahlížení do zdravotnické dokumentace neoprávněným osobám. Poskytovatel se zavazuje zajistit informovanost svých pracovníků o povinnostech vyplývajících z této smlouvy. Poskytovatel se zavazuje zajistit, aby jeho pracovníci, kteří budou přicházet do styku s Osobními údaji, byli smluvně vázáni povinností mlčenlivosti ve smyslu Nařízení a Zákona o zpracování osobních údajů a poučeni o možných následcích porušení těchto povinností s tím, že povinnost důvěrnosti bude jimi dodržována i po skončení jejich smluvního vztahu k Poskytovateli. Poskytovatel prohlašuje, že jeho zaměstnanci a/nebo subdodavatelé přicházející při výkonu své práce do styku s Osobními údaji Klientů objednatele, byli náležitě poučeni o povoleném způsobu nakládání s Osobními údaji a byli seznámeni s následky jednání, které by bylo v rozporu se zákonnou úpravou a bezpečnostními směrnicemi objednatele, s nimiž byli prokazatelně seznámeni.
11. Poskytovatel zajišťuje bezpečné zpracování Osobních údajů Klientů objednatele zejména následujícími organizačními a technickými opatřeními Poskytovatele:
    a) Řízením jednoznačně identifikovatelného a zabezpečeného přístupu zaměstnanců a/nebo subdodavatelů Poskytovatele k IS Objednatele,
    b) Aplikací kryptografických opatření na ochranu Osobních údajů objednatele, v rámci ukládání dat objednatele včetně elektronické komunikace v rámci veřejné sítě internet,
    c) Aplikací systému zaznamenávání a vytváření záznamů událostí a změn formou logů.
12. Osobní údaje nebudou poskytnuty ani jakkoliv zpřístupněny třetím osobám ze zemí mimo EU a EHP.

13. Poskytovatel je povinen informovat objednatele bez zbytečného odkladu o zapojení dalšího zpracovatele, sdělit jeho identifikační údaje, a to s dostatečným předstihem tak, aby měl objednatel možnost vyslovit vůči této změně své oprávněné námitky.

14. Poskytovatel tímto prohlašuje, že v rámci své činnosti implementoval požadavky Nařízení a zpracování Osobních údajů bude probíhat v souladu s pravidly Nařízení. Poskytovatel se zejména zavazuje:

    a) zpracovávat Osobní údaje pouze na základě doložených pokynů objednatele činěného prostřednictvím oprávněných osob podle ujednání a způsobem dle této smlouvy, tedy výhradně pokynem v písemné podobě prostřednictvím informačního systému datových schránek anebo prostřednictvím záznamu do zákaznického portálu Poskytovatele na adrese https://www.gemsupport.cz, přičemž doloženého pokynu objednatele je třeba i tehdy, mají-li být Osobní údaje předávány do třetí země nebo mezinárodní organizaci; Poskytovatel je povinen archivovat veškeré pokyny objednatele,

    b) zachovávat mlčenlivost o povaze a nakládání s Osobními údaji,

    c) provést vhodná technická a organizační zabezpečení, aby zajistil úroveň zabezpečení odpovídající danému riziku, při posuzování vhodné úrovně zabezpečení Poskytovatel zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných Osobních údajů, nebo neoprávněný přístup k nim,

    d) nepředat ani nezpřístupnit Osobní údaje žádné třetí osobě, s výjimkami sjednanými výše (viz další zpracovatel) bez předchozího písemného souhlasu objednatele, tedy nezapojit do zpracování žádného dalšího zpracovatele bez předchozího písemného povolení objednatele, udělí-li objednatel povolení k zapojení dalšího zpracovatele, musí být tomuto dalšímu zpracovateli uloženy stejné povinnosti na ochranu Osobních údajů, jaké jsou uvedeny v tomto článku smlouvy,

    e) zohlednit povahu zpracování a být objednateli nápomocen prostřednictvím vhodných technických a organizačních opatření při plnění objednatelovy povinnosti reagovat na žádosti o výkon práv subjektů údajů stanovených v kapitole III. Nařízení (Práva subjektu údajů),

    f) být objednateli nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36 Nařízení, zejména být nápomocen v případech porušení zabezpečení Osobních údajů k tomu, aby objednatel mohl vyhodnotit, zda porušení mělo za následek riziko pro práva a svobody Klientů, případně být nápomocen k tomu, aby objednatel mohl řádně a včas ohlásit porušení zabezpečení Osobních údajů dozorovému úřadu (včetně údajů dle čl. 33 odst. 3 Nařízení) a ohlásit to Klientům, při výkonu této povinnosti je Poskytovatel povinen reagovat bez zbytečného odkladu na pokyny a požadavky objednatele, a to při zohlednění povahy zpracování a informací, jež má Poskytovatel k dispozici,

    g) ohlásit objednateli případy porušení zabezpečení Osobních údajů bez zbytečného odkladu, nejpozději do 24 hod hodin od zjištění porušení,

    h) poskytnout objednateli veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v tomto článku a umožnit audity, včetně inspekcí, prováděné objednatelem nebo jiným auditorem, kterého objednatel pověřil, a poskytovat součinnost k těmto auditům,

    i) neprodleně informovat objednatele v případě, že podle názoru Poskytovatele určitý pokyn objednatele porušuje ustanovení Nařízení nebo jiné předpisy týkající se ochrany Osobních údajů.

15. Zodpovědné kontaktní osoby pro problematiku zajištění ochrany osobních údajů vyplývající z této smlouvy jsou uvedeny v příloze č. 2 Smlouvy.

Článek 11
Kybernetická bezpečnost

1. Poskytovatel tímto bere na vědomí, že Objednatel je osobou povinnou dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „ZoKB“) a plní povinnosti vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „VyKB“).

2. Poskytovatel tímto bere na vědomí, že je pro Objednatele při zajišťování smluvního vztahu založeného touto smlouvou v pozici významného dodavatele ve smyslu § 2 odst. n) VyKB.
3. Objednatel je v souladu s ustanovením § 4 odst. 4 ZoKB a ve spojení s přílohou č. 7 VyKB povinen stanovit závazná bezpečnostní opatření, která se vztahují na Poskytovatele při plnění předmětu této smlouvy (dále jen „Bezpečnostní opatření“).
4. Poskytovatel je povinen v rozsahu plnění této Smlouvy naplnit všechna Bezpečnostní opatření uvedená v příloze č. 4 – Bezpečnostní požadavky.
5. Poskytovatel umožní Objednateli v roční periodě po dobu účinnosti této Smlouvy provedení zákaznického auditu (kontroly). Předmětem bude naplnění Bezpečnostních opatření. Objednatel je oprávněn při auditu (kontrole) využít třetí stranu.
6. Poskytovatel umožní Objednateli kontrolu Bezpečnostních požadavků provedenou prostředky Objednatele nebo třetí stranou, a to v lokalitě Poskytovatele i vzdáleně, pokud to technické prostředky Poskytovatele umožňují.
7. Poskytovatel se zavazuje poskytnout Objednateli součinnost minimálně v rozsahu patnáct (5) člověkodní při provádění každého auditu (kontroly) ze strany Objednatele a pro tuto činnost zajistit účast kvalifikovaných pracovníků.
8. Poskytovatel se zavazuje nedostatky zjištěné na základě provedeného auditu (kontroly) dle odst. 6 odstranit ve lhůtě určené v písemném oznámení Objednatele. Nestanoví-li Objednatel lhůtu v písemném oznámení, zavazuji se Smluvní strany dohodnout na lhůtě pro odstranění nedostatku, která nepřevýší 90 kalendářních dnů.
9. Poskytovatel se dále zavazuje:
    a) poskytnout na vyžádání Objednateli dokumenty, zprávy, a obdobné vstupy, které budou prokazovat naplnění Bezpečnostních požadavků;
    b) na požádání s Objednatelem konzultovat kdykoli v průběhu účinnosti této Smlouvy detailní nastavení bezpečnostních opatření k naplnění Bezpečnostních požadavků a pro takovéto konzultace zajistit účast kvalifikovaných pracovníků;
    c) neprodleně informovat Objednatele o všech významných změnách v naplnění Bezpečnostních požadavků, které nastanou kdykoli v průběhu účinnosti této Smlouvy;
    d) bezodkladně a s vyvinutím nejlepšího úsilí zajistit náhradní způsob naplněné Bezpečnostních požadavků, pokud stávajících řešení přestalo být funkční a efektivní;
    e) bezodkladně a prokazatelně informovat Objednatele o kybernetických bezpečnostních událostech a incidentech, které mohou ovlivnit poskytování služeb dle této Smlouvy;
    f) při výkonu své činnosti včas a prokazatelně upozornit Objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahujících se k Bezpečnostním opatřením a jejichž následkem může vzniknout újma nebo nesoulad s platnými a účinnými právními předpisy či jinými předpisy vztahujícími se k poskytování služeb dle této Smlouvy.
10. Poskytovatel bere na vědomí, že veškeré aktivity Poskytovatele a jeho plnění realizované v prostředí Objednatele mohou být monitorovány a vyhodnocovány v rozsahu předmětu plnění.
11. Zodpovědné kontaktní osoby pro problematiku zajištění kybernetické bezpečnosti vyplývající z této Smlouvy jsou uvedeny v příloze č. 2 této Smlouvy.

Článek 12
Sankce

1. V případě, že Poskytovatel nedodrží časové limity dle přílohy č. 1 pro reakci na zadaný servisní požadavek s prioritou „Havarijní“ (dle přílohy č. 1 této smlouvy), aniž by to bylo způsobeno neplněním povinností a smluvních závazků ze strany Objednatele nebo okolnostmi vylučujícími odpovědnost, uhradí Poskytovatel Objednateli na základě faktury smluvní pokutu ve výši 1000,- Kč za každých započatých 15 minut prodlení.
2. V případě, že Poskytovatel nedodrží časové limity dle přílohy č. 1 pro reakci na zadaný servisní požadavek s prioritou „Vysoká“ (dle přílohy č. 1 této smlouvy), aniž by to bylo způsobeno neplněním povinností a smluvních závazků ze strany Objednatele nebo okolnostmi vylučujícími odpovědnost, uhradí Poskytovatel Objednateli na základě faktury smluvní pokutu ve výši 1000,- Kč za každých započatých 30 minut prodlení.

3. V případě nezaplacení faktur Objednatelem na účet Poskytovatele v termínu splatnosti bude Poskytovatelem uplatněn úrok z prodlení ve výši 0,01% z celkové fakturované částky za každý den prodlení.
4. V případě prodlení plateb Poskytovatelem na účet Objednatele bude Objednatelem uplatněn úrok z prodlení ve výši 0,01% z celkové fakturované částky za každý den prodlení.
5. Za prokázané porušení povinností o ochraně informací či zneužití dat ve smyslu čl. 9 a 10 této smlouvy má poškozená strana právo požadovat po druhé smluvní straně smluvní pokutu ve výši 500.000,- Kč za každé porušení povinností o ochraně informací ve smyslu čl. 9 této smlouvy.
6. Za prokázané porušení povinností Poskytovatele v oblasti kybernetické bezpečnosti dle čl. 11 této smlouvy nebo bezpečnostních požadavků uvedených v příloze č. 4 této smlouvy uhradí Poskytovatel Objednateli smluvní pokutu ve výši 50.000,- Kč (slovy: padesát tisíc korun českých) za každý jednotlivý případ porušení výše uvedených povinností Poskytovatele.
7. Sankce, sjednané touto smlouvou, hradí povinná strana nezávisle na tom, zda a v jaké výši vznikne druhé straně v této souvislosti škoda, kterou lze vymáhat samostatně.
8. Započtení závazků a pohledávek vyplývajících z ustanovení této smlouvy je možné pouze na základě písemného souhlasu druhé smluvní strany.
9. Uhrazením jakékoliv sjednané smluvní pokuty není dotčeno právo na náhradu škody.

Článek 13
Platnost a účinnost smlouvy

1. Tato smlouva se uzavírá na dobu určitou, a to 2,5 roku (tj. 30 měsíců) od 1.7.2022 do 31.12.2024.
2. Objednatel i Poskytovatel mohou Smlouvu vypovědět kdykoliv s šestiměsíční výpovědní lhůtou bez udání důvodu. Výpovědní lhůta začíná běžet 1. den měsíce následujícího po doručení výpovědi druhé smluvní straně.
3. Smlouvu lze také předčasně ukončit dohodou smluvních stran nebo odstoupením od Smlouvy.
4. Poskytovatel i Objednatel jsou oprávněni od této Smlouvy odstoupit ze zákonných důvodů, a dále zejména v případech podstatného porušení této Smlouvy sjednaných touto Smlouvou v bodech 5. a 6. tohoto článku Smlouvy. Odstoupení musí být učiněno písemnou formou, musí obsahovat důvody odstoupení a musí být doručeno druhé smluvní straně. Účinky odstoupení vznikají dnem doručení odstoupení druhé smluvní straně.
5. Za podstatné porušení Smlouvy na straně Poskytovatele se zejména považuje:
    a) opakované nedodržování stanovených limitů pro reakci na zadané nestandardní stavy a servisní požadavky
    b) opakované porušení povinností o ochraně informací či zneužití dat ve smyslu čl. 9 a 10 Smlouvy
6. Za podstatné porušení Smlouvy na straně Objednatele se zejména považuje:
    a) prodlení s plněním peněžitých závazků po dobu delší než čtrnáct (14) dní od prokazatelného doručení písemného upozornění Poskytovatele
    b) neposkytování potřebné součinnosti pro plnění dle této Smlouvy po dobu delší než pět (5) dní od prokazatelného doručení písemného upozornění Poskytovatele.
7. Odstoupením od Smlouvy nejsou dotčena ustanovení týkající se smluvních pokut, úroků z prodlení, ochrany informací, řešení sporů a ustanovení týkající se těch práv a povinností, z jejichž povahy vyplývá, že mají trvat i po odstoupení od Smlouvy.

Článek 14
Závěrečná ustanovení

1. Tato smlouva nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti dnem 1.7.2022 s podmínkou předchozího uveřejnění Smlouvy prostřednictvím Registru smluv. Pokud bude smlouva uveřejněna po 1.7.2022, tak je účinná dnem uveřejnění.
2. Tato smlouva je vyhotovena v jednom stejnopise v elektronické podobě a podepsána elektronickým podpisem dle zák. č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

3. Tato smlouva může být měněna dohodou smluvních stran písemnými dodatky podepsanými oprávněnými osobami. Smluvní strany se zavazují podílet se na případných změnách smlouvy bez zbytečných průtahů.
4. Smluvní strany tímto prohlašují, že se dohodly na místní příslušnosti soudu v souladu s ustanovením § 89a zákona č. 99/1963 Sb., občanský soudní řád v platném znění takto: Místně příslušným soudem pro případ sporů vyplývajících z této smlouvy je soud příslušný dle sídla Objednatele.
5. Právní vztahy smluvních stran neupravené touto smlouvou se řídí ustanoveními zákona č. 89/2012 Sb., občanského zákoníku, jakož i ustanoveními dalších obecně závazných právních předpisů. Toto ustanovení se týká i místní příslušnosti soudů v případě soudního sporu vedeného smluvními stranami ohledně vztahů upravených touto smlouvou.
6. Nedílnou součástí této smlouvy jsou následující přílohy:

   Příloha č. 1 – Rozsah podpory
   Příloha č. 2 – Seznam oprávněných osob
   Příloha č. 3 – Detailní rozpis ceny plnění
   Příloha č. 4 – Bezpečnostní požadavky
   Příloha č. 5 – Podmínky pro přístup Poskytovatele do vnitřní sítě FN Plzeň prostřednictvím VPN

V …… dne ……

……

poskytovatel

V …… dne ……

……..

objednatel

Příloha č. 1 Smlouvy o poskytování servisních služeb č. 812/22/13/SIS
Rozsah podpory

Článek 1
Podporované prostředí

Prostředí, k němuž jsou vztaženy servisní služby poskytované dle této smlouvy, se skládá z:

a) 2 primárních serverů Oracle EE v konfiguraci Real Application Cluster (dále jen RAC), které jsou umístěny v různých serverovnách

b) 1 DataGuard Oracle EE serveru v jiné lokalitě

c) 2 testovacích Oracle EE serverů v RAC

d) 2 servery Oracle SE2 v konfiguraci active/passive s aplikační vazbou na servery z bodu a) tohoto článku

Článek 2
Podpora provozu

Podpora provozu zahrnuje:

a) Správu OS RedHat, vč. odstraňování provozních problémů (pro servery uvedené v bodech a) a b) čl. 1 této přílohy) v režimu 24x7x365 – tedy nepřetržitě, 24 hodin denně, 7 dní v týdnu, 365 dní v roce

b) Správu db prostředí Oracle EE, vč. odstraňování provozních problémů (pro stejné servery a ve stejném režimu jako v bodu a) tohoto článku)

c) Správu db prostředí Oracle EE, vč. odstraňování provozních problémů (pro servery uvedené v bodu c) čl. 1 této přílohy) v režimu 8x5 – tedy v pracovní dny, v době od 8.00 do 16.00 hodin

d) Správu db prostředí Oracle SE, vč. odstraňování provozních problémů (pro servery uvedené v bodu d) čl. 1 této přílohy) v režimu 24x7x365 – tedy nepřetržitě, 24 hodin denně, 7 dní v týdnu, 365 dní v roce

e) Min. 2x ročně instalaci patchů OS (pro servery uvedené v bodech a) a b) čl. 1 této přílohy) a db prostředí (pro všechny servery uvedené v čl. 1 této přílohy)

f) Instalaci relevantních bezpečnostních patchů OS a db, kdykoli budou vydány pro provozované prostředí

g) Průběžné kontroly výkonnosti Oracle EE i SE2 řešení (databáze, servery, disková pole), vč. návrhů na zlepšení, a spolupráci při odstraňování chybových stavů.

Článek 3
Service Level Agreement (SLA)

Služba spočívá v řešení nestandardních stavů podporovaného prostředí Oracle a servisních požadavků. HelpDeskový portál pro hlášení nestandardních stavů a servisních požadavků i servisní telefon HotLine pro hlášení nestandardních stavů a služba reakce na nestandardní stavy a servisní požadavky dle níže uvedených priorit je zajištěna nepřetržitě, 24 hodin, 7 dní v týdnu. 365 dní v roce.

Pro zadávání servisních požadavků jsou stanoveny priority:

1. Havarijní – Systém je postižen závadou, která znemožňuje plnohodnotnou práci více než 10% uživatelů (zahrnuje i nestandardní odezvy). Je ohrožena bezpečnost systému.
2. Vysoká – všechny incidenty, které nespadají do kategorie Havarijní a mají dopad na koncové uživatele.
3. Standardní – incidenty nespadající do kategorií Havarijní, Vysoká, včetně servisních a změnových požadavků.

Poskytovatel se zavazuje k nástupu na řešení servisního požadavku s danou prioritou a jeho vyřešení takto:

1. Havarijní – Nástup na řešení požadavku bezodkladně po jeho nahlášení, nejpozději do 15 minut v režimu 24x7x365, odstranění v nejkratší možné době, nejpozději do 2 hodin

2. Vysoká – Nástup na řešení požadavku bezodkladně po jeho nahlášení, nejpozději do 30 minut v režimu 24x7x365, odstranění v nejkratší možné době, nejpozději do 4 hodin
3. Standardní – Nástup na řešení požadavku bezodkladně po jeho nahlášení, nejpozději do 2 hodin v režimu 24x7x365, odstranění v nejkratší možné době, nejpozději do 12 hodin pro incidenty nebo dle dohody obou smluvních stran pro servisní a změnové požadavky

Vyřešením požadavku se rozumí:

- vyřešení nahlášeného požadavku nebo
- přepnutí na DataGuard pro servery uvedené v bodu a) čl. 1 této přílohy nebo
- přepnutí na Passive pro servery uvedené v bodu d) čl. 1 této přílohy nebo
- postoupení problému k vyřešení třetí osobě (Oracle, dodavatel KIS) v případě problému vyvolaného nekorektním chováním komponenty dodané nebo podporované třetí osobou a navržení přijatelného náhradního řešení (workaround)

Článek 4
Nepřetržitý monitoring

Služba spočívá v nepřetržitém dohledu nad provozem realizovaném vzdáleně z dohledového centra dodavatele v režimu 24x7x365, neprodleném vyrozumění odpovědných zaměstnanců Objednatele o problematických stavech a neprodleném zahájení řešení těchto stavů samostatně nebo ve spolupráci s Objednatelem, resp. poskytování konzultací Objednateli k těmto stavům.

Příloha č. 2 Smlouvy o poskytování servisních služeb č. 812/22/13/SIS
Seznam oprávněných osob

Oprávněné osoby Objednatele:

Jméno a příjmení	Ve věcech	Telefon	Email

Oprávněné osoby Poskytovatele:

Jméno a příjmení	Ve věcech	Telefon	Email

Příloha č. 3 Smlouvy o poskytování servisních služeb č. 812/22/13/SIS
Detailní rozpis ceny plnění

Poskytovaná služba	Cena služby bez DPH (za období 1 měsíc)	Celková cena služby bez DPH(za 2,5 roku, tj. 30 měsíců)
Podpora provozu	36 400 Kč	1 092 680 Kč
Nepřetržitý monitoring	19 600 Kč	588 000 Kč
Měsíční platba	**56 000 Kč**	
Celková cena za 2,5 roku trvání smlouvy		**1 680 000 Kč**

Příloha č. 4 Smlouvy o poskytování servisních služeb č. 812/22/13/SIS

Bezpečnostní požadavky

Článek 1

Úvod

1. Tato příloha č. 4 Smlouvy popisuje bezpečnostní požadavky kladené na Poskytovatele v rámci realizace veřejné zakázky „Podpora provozu Oracle Enterprise Edition a nepřetržitý dohled nad provozem v období červenec 2022 – prosinec 2024 “, zejména pro naplnění požadavků vyplývajících pro Poskytovatele ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZoKB“), a 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 jen „VyKB“).
2. Poskytovatel je povinen plnit relevantní povinnosti v rozsahu a způsobem, aby byl naplněn účel právní úpravy oblasti bezpečnostních opatření kybernetické bezpečnosti ve vztahu k povinnostem, které tato právní úprava stanovuje Objednateli jakožto povinné osobě dle ZoKB. V takovém případě je Objednatel oprávněn požadovat od Poskytovatele přiměřenou součinnost i nad rámec povinností stanovených v této příloze, avšak vždy pouze za účelem zajištění plnění povinnosti Poskytovatele z oblasti kybernetické bezpečnosti ve smyslu shora uvedeného.

Článek 2

Bezpečnostní požadavky

2.1. Účel

1. Tato příloha Smlouvy stanoví způsoby a úrovně realizace bezpečnostních opatření pro Poskytovatele a určuje vzájemný vztah odpovědnosti za zavedení a kontrolu bezpečnostních opatření mezi Objednatelem a Poskytovatelem. Požadavky na Poskytovatele jsou definovány dle platné právní úpravy, především pak dle ZoKB, VyKB.
2. Smluvní strany se dohodly, že pokud to bude potřebné ke splnění požadavků ZoKB, VyKB, či souvisejících právních předpisů z oblasti bezpečnosti informací, uzavřou bez zbytečného odkladu po výzvě kterékoli smluvní strany písemný dodatek Smlouvy zohledňující takové požadavky.

2.2. Obecné požadavky

1. Poskytovatel se při poskytování plnění pro Objednatele zavazuje plnit následující povinnosti:
    a) postupovat v souladu s účinnými právními předpisy, zejména pak požadavky vyplývajícími pro Poskytovatele, jakožto významného dodavatele provozovatele základní služby, ze ZoKB, VyKB a reflektovat případné novely dotčených právních předpisů či novou právní úpravu;
    b) dodržovat příslušná ustanovení bezpečnostních politik, metodik a postupů předaných Poskytovateli Objednatelem, resp. platné řídící dokumentace Objednatele či její části anebo platné řídící dokumentace, k jejímuž dodržování se Objednatel zavázal, pokud byl Poskytovatel s takovými dokumenty nebo jejich částmi seznámen, a to bez ohledu na způsob, jakým byl s takovou dokumentací Objednatele seznámen (např. školením, protokolárním předáním příslušné dokumentace poskytovateli, elektronickým předáním prostřednictvím e-mailu, zřízením přístupu Poskytovateli na sdílené úložiště aj.);
    c) rozvíjet bezpečnostní povědomí svých zaměstnanců a příp. dalších osob, které se podílejí na plnění Smlouvy a průběžně je seznamovat s prováděnými nebo plánovanými změnami. Zaměstnanci a další osoby na straně Poskytovatele podílející se na plnění Smlouvy musí být prokazatelně seznámeni s platnými předpisy a bezpečnostními požadavky Objednatele, a to

ještě před zahájením jakékoli činnosti ze strany těchto osob pro Objednatele v souvislosti s plněním této Smlouvy;

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

e) přidělovat svým jednotlivým zaměstnancům oprávnění k výkonu činností a dodržovat při tom bezpečnostní zásadu tzv. „potřeba vědět“ (need-to-know principle), tedy zejména dbát o to, aby byla minimalizována rizika nežádoucího přístupu k aktivům Objednatele;

f) průběžně dokumentovat, kontrolovat a vyhodnocovat oprávněnost přístupu, jak fyzického, tak i logického, u všech osob na straně Poskytovatele, které přistupují k předmětu plnění dle této Smlouvy;

g) průběžně detekovat technické zranitelnosti a konfigurační nesoulady předmětu plnění Smlouvy a o zjištěných skutečnostech bez zbytečného odkladu informovat Objednatele. Detekované technické zranitelnosti musí být vyhodnoceny s ohledem na související riziko a musí podle povahy předmětu plnění dojít k nápravným opatřením ze strany Poskytovatele. Nápravná opatření musí být schválena Objednatelem;

h) realizovat bezpečnostní opatření pro ochranu dat souvisejících s plněním předmětu Smlouvy.

2.3. Bezpečnost informací

1. Poskytovatel je povinen zajistit utajení získaných důvěrných informací objednatele způsobem obvyklým pro utajování takových informací, není-li výslovně sjednáno jinak. Tato povinnost platí bez ohledu na ukončení účinnosti této smlouvy. Poskytovatel je povinen zajistit utajení důvěrných informací i u svých zaměstnanců, zástupců, jakož i jiných spolupracujících třetích stran, pokud jim takové informace byly poskytnuty.
2. Právo užívat, poskytovat a zpřístupnit důvěrné informace má Poskytovatel pouze v rozsahu a za podmínek nezbytných pro řádné plnění práv a povinností vyplývajících z této Smlouvy.
3. Za důvěrné informace se bez ohledu na formu jejich zachycení považují veškeré informace, které nebyly Objednatelem označeny jako veřejné a které se týkají této Smlouvy a jejího plnění (zejména informace o právech a povinnostech smluvních stran jakož i informace o cenách a systémových konfiguracích a infrastruktuře), které se týkají Objednatele, jeho smluvních partnerů, pacientů, obchodní tajemství, anebo informace pro nakládání, s nimiž je stanoven právními předpisy zvláštní režim utajení. Dále se považují za důvěrné informace takové informace, které jsou jako důvěrné výslovně Objednatelem označeny.
4. Za důvěrné informace se v žádném případě nepovažují informace, které se staly veřejně přístupnými, pokud se tak nestalo porušením povinnosti jejich ochrany, dále informace získané na základě postupu nezávislého na této Smlouvě a informace poskytnuté třetí osobou, která takové informace nezískala porušením povinnosti jejich ochrany.
5. Poskytovatel je povinen zajistit bezpečnost informací z pohledu dostupnosti. Informace se z pohledu dostupnosti považují za bezpečné, jestliže jsou dostupné autorizovaným uživatelům v době, kdy jsou potřeba.
6. Poskytovatel je povinen zajistit bezpečnost informací z pohledu integrity. Informace se z pohledu integrity považují za bezpečné, jestliže je zaručena jejich správnost, bezchybnost a jsou vyloučeny jejich neautorizované změny.

2.4. Oprávnění užívat data

1. Poskytovatel je při poskytování plnění pro Objednatele oprávněn užívat informace předaná Poskytovateli Objednatelem za účelem plnění předmětu Smlouvy, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu Smlouvy.
2. Poskytovatel se při poskytování plnění pro Objednatele zavazuje nakládat s informacemi pouze v souladu se Smlouvou a příslušnými právními předpisy, zejména ZoKB, VyKB a dalšími souvisejícími právními předpisy.

2.5. Řetězení a řízení dodavatelů

1. Poskytovatel nezapojí do poskytování plnění dle této Smlouvy žádného dalšího poddodavatele bez předchozího konkrétního nebo obecného písemného povolení Objednatele.
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.
3. Poskytovatel je povinen předat Objednateli kontaktní údaje všech osob dodávajících systémovou a technickou podporu pro řešení.
4. Pokud Poskytovatel využívá při poskytování plnění poddodavatele, zavazuje se, že budou dodržovat bezpečnostní požadavky vč. požadavků na ochranu osobních údajů vyplývající z této Smlouvy.
5. Poskytovatel se zavazuje bezodkladně doložit Objednateli na základě jeho výzvy smluvní dokumenty se svými poddodavateli, ze kterých bude vyplývat závazek poddodavatele poskytovat plnění v souladu s bezpečnostními požadavky vyplývajícími z této Smlouvy.
6. Poskytovatel odpovídá za to, že jeho poddodavatelé nebudou jednat v rozporu s bezpečnostními požadavky vyplývajícími z této Smlouvy.

2.6. Řízení změn

1. Poskytovatel se zavazuje provést hodnocení dopadů Objednatelem navrhovaných změn na termíny a cenu předmětu plnění Smlouvy. Pokud by však takovéto hodnocení vyžadovalo dodatečné náklady anebo by nepříznivě ovlivnilo pracovní vytížení zaměstnanců nebo využití jiných prostředků určených k provádění předmětu plnění, Poskytovatel tuto skutečnost oznámí Objednateli a hodnocení provede pouze na základě písemného pověření Objednatelem. V takovém případě bude hodnocení hrazeno podle stráveného času v sazbách platných v době hodnocení.
2. Poskytovatel 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 informačního systému a zajistí možnost navrácení do původního stavu.
3. Poskytovatel má povinnost informovat Objednatele o výsledcích řízení změn, které mají dopady na plnění předmětu Smlouvy ze strany Poskytovatele.
4. Poskytovatel má povinnost přijmout účinná opatření ke snížení nepříznivých dopadů v souladu s výsledky řízení změn
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. V případě realizace penetračního testování nebo testování zranitelnosti řešení poskytne Poskytovatel Objednateli veškerou potřebnou součinnost.

2.7. Zvládání kybernetických bezpečnostních událostí a incidentů

1. Poskytovatel se při poskytování plnění pro Objednatele zavazuje v rozsahu poskytovaných služeb dle Smlouvy, že:
    a) stanoví činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání kybernetických bezpečnostních událostí a incidentů, podle takto stanovených a popsaných pravidel bude postupovat, a bude hlásit všechny bezpečnostní události a incidenty neprodleně po jejich detekci Objednateli prostřednictvím ohlašovacích kanálů na osobu odpovědnou za kybernetickou bezpečnost, v případech, kdy situace nestrpí odklad telefonicky;
    b) nastavená pravidla pro zvládání bezpečnostních incidentů budou respektovat požadavek na legalitu zajištění stop, tj. jejich původ a oprávněnost jejich získaní musí být v souladu

s platnými zákony a standardy tak, aby bylo možné jejich následné využití v rámci forenzní analýzy a eventuální použití jako důkazní materiál;

c) navrhne řešení tak, aby byl systém detekce a zvládání bezpečnostních událostí a incidentů začleněn do procesů a systémů a realizuje opatření pro zvýšení odolnosti informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti;

d) provede analýzu příčin bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování v případě, že Poskytovatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

2.8. Informační povinnost a povinnosti při výměně informací

1. Poskytovatel se během poskytování plnění pro Objednatele zavazuje Objednatele informovat o:
    a) způsobu řízení rizik, zbytkových rizicích souvisejících s plněním Smlouvy a bez zbytečného odkladu také o změnách ve způsobu řízení rizik;
    b) změně vlastnictví zásadních aktiv, využívaných Poskytovatelem k plnění Smlouvy, a změně oprávnění nakládat s těmito aktivy, a to nejpozději do tří pracovních dnů po uskutečnění této změny.
2. Poskytovatel se během poskytování plnění pro Objednatele zavazuje dostatečně zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost.

2.9. Řízení kontinuity činností

1. Objednatel má oprávnění zapojit Poskytovatele do řízení kontinuity činností, a to zejména oprávnění k zahrnutí Poskytovatele do plánu kontinuity činností, který souvisí s informačním systémem a souvisejících služeb a/nebo zahrnutí Poskytovatele do Plánu obnovy (DRP) Objednatele.
2. Objednatel má povinnost informovat Poskytovatele o způsobu zapojení do řízení kontinuity činností.

2.10. Bezpečnost lidských zdrojů

1. Poskytovatel zajistí poučení všech svých zaměstnanců podílejících se na dodávce o bezpečnostních pravidlech uvedených v těchto Bezpečnostních požadavcích, jež se musí v průběhu dodávky dodržovat a zajistí jejich dodržování nasazením kontrolních a vynucovacích mechanismů. Rozsah poučení podléhá schválení Objednatele osobou určenou za kybernetickou bezpečnost.
2. Poskytovatel se zaváže zajistit dostatečnou míru zastupitelnosti pro technické aspekty řešení (zajištění kontinuity dodávky, zastupitelnost zaměstnanců).
3. Poskytovatel je povinen vést písemnou evidenci uskutečněných poučení v rozsahu předmět poučení, datum a seznam poučených osob. Poskytovatel se zavazuje předložit tuto evidenci objednateli bezodkladně poté, co k tomu bude Objednatelem vyzván.

2.11. Bezpečnost komunikace

1. Zaměstnanci Poskytovatele, kteří mají přidělen přístup do interní sítě FN Plzeň (většinou na konkrétní server), odpovídají za své činnosti prováděné v rámci interní sítě FN Plzeň. Z důvodu zajištění bezpečnosti zaměstnanci Poskytovatele nesmí zejména:
    a) zneužívat síťové prostředky pro osobní účely a zatěžovat kapacitu sítě;
    b) šířit škodlivý kód;
    c) připojovat do sítě jiná, než schválená zařízení Poskytovatelem (včetně USB zařízení, soukromých mobilních zařízení, IoT zařízení apod.);
    d) využívat nástroje sloužící k maskování identity;
    e) provádět bezdůvodné skenování portů;

f) provádět jakoukoliv formou monitorování počítačoví sítě, které může vést k zachycení informací/dat, pokud není předmětem plnění smlouvy;

g) obcházet autentizaci uživatele nebo obcházet zabezpečení jakéhokoliv počítače, počítačové nebo zdravotnické sítě;

h) provádět jakékoliv nepracovní aktivity vedoucí k omezování nebo odepírání služeb jiným uživatelům;

i) 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 počítačovou síť, internet nebo intranet;

j) využívat bezpečnostních mezer nebo vytvářet útoky na komunikaci v počítačových sítích (např. přístup k datům, jichž není zaměstnanec zamýšleným příjemcem, přihlašování na server nebo účet zaměstnancem, který není k tomuto přístupu výslovně oprávněn, s výjimkou případů, kdy tyto aktivity jsou součástí řádných pracovních úkolů);

k) předávat informace o konfiguraci a topologii sítě cizím osobám; tyto informace je oprávněn předat pouze odpovědný zaměstnanec FN Plzeň, pokud jsou takové informace nutné z hlediska přípravy či plnění smluvního vztahu.

2. Při práci na pracovní stanici, mobilním zařízení připojeného do sítě nebo do informačního systému FN Plzeň musí Poskytovatel dodržovat tyto základní zásady:

   a) umožnit přístup jen poučenému zaměstnanci Poskytovatele;

   b) chránit ICT prostředky FN Plzeň;

   c) po ukončení práce provést neprodleně odhlášení tak, aby se zamezilo zneužití jeho přístupových práv.

2.12. Řízení přístupu

1. Poskytovatel bere na vědomí, že přístup k datům, informacím či zařízením souvisejícím s předmětem Smlouvy je možné povolit pouze fyzické identitě zaměstnance Poskytovatele poučené o těchto Bezpečnostních požadavcích, a to na základě požadavku Poskytovatele na přístup.
2. Poskytovatel bere na vědomí, že přidělení oprávnění zaměstnanci Poskytovatele musí být řízeno zásadou tzv. „potřeba vědět“ (need-to-know principle) a není nárokové.
3. Poskytovatel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci Poskytovatele.
4. Poskytovatel se zavazuje, že nebude instalovat a používat žádné nástroje, které nebyly předem písemně odsouhlaseny osobou odpovědnou za kybernetickou bezpečnost na straně Objednatele a jejichž užívání by mohlo ohrozit kybernetickou bezpečnost.
5. Poskytovatel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části technologického nebo komunikačního systému programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci technologického nebo komunikačního systému nebo nelegální získání dat a informací. Poskytovatel bere na vědomí, že přístup do interní sítě a/nebo k technologickým a komunikačním systémům bude realizován výhradně s využitím zařízení Objednatele.
6. Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli, kteří přistupují do interní sítě a/nebo technologického nebo komunikačního systému chránili autentizační prostředky a údaje k systémům Objednatele. Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako bezpečnostní incident ve smyslu příslušné řídící dokumentace a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu.
7. Poskytovatel se zavazuje, že nebude instalovat a používat zejména nástroje typu Keylogger, Sniffer, Analyzátor zranitelností a Port Scanner, Backdoor, rootkit a trojský kůň nebo jinou podobu malware.
8. Poskytovatel bere na vědomí, že postup zvládání bezpečnostního incidentu či skutečnost vzniklá v důsledku porušení bezpečnostních požadavků nebude posuzována 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.
9. Na základě smluvního vztahu může být konkrétním zaměstnancům Poskytovatele umožněn přístup k předmětným ICT prostředkům pomocí vzdáleného přístupu přes VPN. Pracovní stanice, přenosná

zařízení zaměstnanců Poskytovatele přistupující k ICT prostředkům Objednatele musí mít instalován výrobcem podporovaný aktualizovaný operační systém a systém pro ochranu před škodlivým kódem (antivirový program) s nejnovější verzí virové databáze.

10. Lokální přístup Poskytovatele do provozního prostředí může být povolen pouze v odůvodněných případech. Tento přístup musí probíhat ve zvláštním režimu dohledu ze strany SIS.)

2.13. Ochrana před škodlivým kódem

1. Poskytovatel se zavazuje, že zajistí maximální ochranu před zavlečením škodlivého SW do interní sítě Objednatele. Zaměstnanci, resp. subdodavatelé Poskytovatele mají zakázáno používat soukromou výpočetní techniku pro připojování do interní sítě Objednatele.

2.14. Monitorování činností

1. Poskytovatel bere na vědomí, že veškeré aktivity Poskytovatele a jeho plnění realizované v rámci plnění předmětu Smlouvy nebo s ním úzce související budou Objednatelem průběžně a pravidelně monitorovány a vyhodnocovány s ohledem na obsah Smlouvy.

2.15. Kontrola souladu s požadavky bezpečnosti

1. Poskytovatel se zavazuje umožnit Objednateli nebo jím pověřené třetí osobě provést audit plnění povinností Poskytovatele dle této Smlouvy, zejména způsobu plnění bezpečnostních opatření, způsobu řízení dodavatelů, nakládání s daty, způsobu identifikace a hlášení kybernetických bezpečnostních incidentů. Objednatel se zavazuje vyrozumět Poskytovatele o termínu a případně osobě pověřené provedením auditu alespoň 3 pracovní dny předem. Poskytovatel se zavazuje umožnit provedení auditu ve všech prostorách, v nichž dochází k plnění předmětu této Smlouvy. Náklady na uskutečnění auditu ponese každá smluvní strana zvlášť; Poskytovatel nemá právo na poskytnutí úhrady nákladů či jakéhokoliv jiného plnění v souvislosti s auditem. V případě, že výsledkem auditu budou zjištění o pochybeních na straně Poskytovatel, zavazuje se Poskytovatel bezodkladně po výzvě Objednatele veškeré takové nedostatky na své náklady odstranit. Poskytovatel je povinen zajistit umožnění auditu za stejných podmínek i u svých poddodavatelů.
2. Poskytovatel je povinen pravidelně provádět také vlastní hodnocení rizik a kontrolu zavedených bezpečnostních opatření. Tato kontrola probíhá v pravidelných intervalech stanovených Objednatelem, na žádost Objednatele nebo v případě vzniku kybernetického bezpečnostního incidentu v rámci poskytované služby nebo v případě, že se vznik bezpečnostního incidentu jeví jako pravděpodobný. O výsledku kontroly podá Poskytovatel Objednateli bez zbytečného odkladu písemnou kontrolní zprávu.

2.16. Porušení Bezpečnostních požadavků

1. Poskytovatel odpovídá za to, že jeho zaměstnanci a/nebo poddodavatelé nebudou jednat v rozporu s bezpečnostními požadavky vyplývajícími z této Smlouvy. V případě, že dojde k nedodržení těchto požadavků ze strany zaměstnance a/nebo poddodavatele Poskytovatele, považuje se každé takové nedodržení požadavků za porušení povinnosti Poskytovatele dle této Smlouvy.

Příloha č. 5 Smlouvy o poskytování servisních služeb č. 812/22/13/SIS

Podmínky pro přístup Poskytovatele do vnitřní sítě FN Plzeň prostřednictvím VPN FN Plzeň

(dále jen „Podmínky“)

Článek 1

Předmět

Pro zajištění řádného plnění Poskytovatele podle smlouvy, jejíž přílohou jsou tyto Podmínky (dále jen „Smlouva“) a současně za účelem zajištění bezpečnosti vnitřní sítě FN Plzeň, jejích informačních systémů, komunikačních systémů a zdravotnických prostředků (dále jen „informační systém“) jsou těmito Podmínkami stanoveny vzájemné povinnosti smluvních stran, které souvisejí se vzdáleným přístupem Poskytovatele do vnitřní sítě FN Plzeň, informačním systémům a k informacím prostřednictvím VPN FN Plzeň (dále též jen „VPN přístup“).

Za tímto účelem:

1. FN Plzeň zřídí Poskytovateli VPN přístup a zajistí jeho dostupnost po určenou dobu, za podmínek dále uvedených v této příloze.
2. VPN přístup bude Poskytovatelem využíván pouze prostřednictvím osob, které Poskytovatel předem určil a nahlásil správcům VPN FN Plzeň. Tyto osoby se podílejí nebo budou podílet na plnění závazků Poskytovatele podle Smlouvy (dále jen „zaměstnanec Poskytovatele“).
3. VPN přístup bude Poskytovateli zřízen a ponechán pouze v případě, bude-li to pro Poskytovatele nezbytné pro plnění Smlouvy

Článek 2

Zřízení VPN přístupu

1. Zřízením VPN přístupu Poskytovateli se rozumí proces, kterým je zaměstnanci Poskytovatele vytvořen uživatelský účet, pomocí kterého následně může přistupovat, prostřednictvím VPN klienta, do vnitřní sítě FN Plzeň prostřednictvím VPN FN Plzeň.
2. Poskytovatel musí žádat o zřízení VPN prostřednictvím formuláře „Žádost o zřízení/pozastavení/ukončení VPN přístupu Poskytovatele do vnitřní sítě FN Plzeň“ (dále jen „Žádost“), viz Příloha 1. Tato Žádost musí splňovat následující:
    a) každá Žádost je vyplněna pro jednu konkrétní fyzickou osobu. V případě, že Poskytovatel požaduje přístup pro více zaměstnanců, vyplní pro každého z nich vlastní Žádost.
    b) pokud se jedna a tatáž fyzická osoba podílí na plnění podle více smluv uzavřených mezi Poskytovatelem a FN Plzeň, předkládá Poskytovatel FN Plzeň vždy samostatnou Žádost pro zaměstnance Poskytovatele pro každou takovou smlouvu,
    c) anonymní sdílené VPN nejsou povoleny,
    d) Poskytovatel může žádat o VPN přístup maximálně po dobu účinnosti Smlouvy.
3. Takto vyplněnou a podepsanou Žádost zašle Poskytovatel emailem:
    a) Adresa: VPN@fnplzen.cz,
    b) Předmět: VPN přístup “název Poskytovatele“

Žádost musí být podepsaná uznávaným elektronickým podpisem pověřené osoby uvedené ve Smlouvě za Poskytovatele. E-mailovou zprávu zasílá Poskytovatel nejpozději 10 pracovních dnů před datem, od kterého Poskytovatel požaduje zřídit zaměstnanci Poskytovatele VPN přístup.

4. Poskytovatel odpovídá za to, že všechny údaje uvedené v Žádosti jsou správné a platné. V případě, že dojde ke změně některého údaje uvedeného v Žádosti, je Poskytovatel povinen nejpozději do 7 kalendářních dnů od změny předložit novou Žádost s vyznačením požadovaných změn.

5. FN Plzeň doručenou Žádost posoudí z hlediska potřebnosti VPN přístupu pro předmětné plnění Poskytovatele, formálních a věcných náležitostí, případně požádá Poskytovatele o doplnění (opravu) Žádosti.
6. FN Plzeň zašle Poskytovateli a zaměstnanci Poskytovatele prostřednictvím e-mailu informaci o schválení/neschválení Žádosti.
    a) V případě neschválení Žádosti FN Plzeň poskytne zdůvodnění.
    b) V případě schválení Žádosti zasílá FN Plzeň následně na e-mailovou adresu zaměstnance Poskytovatele též informace potřebné pro nastavení VPN přístupu, tj. postup, jakým způsobem se zaměstnanec Poskytovatele připojí do přes VPN do FN Plzeň
7. FN Plzeň zasílá zaměstnanci Poskytovatele na jeho e-mailovou adresu uvedenou v Žádosti přidělené uživatelské jméno a zároveň na jeho mobilní telefonní číslo uvedené v Žádosti heslo.

Článek 3

Pozastavení VPN přístupu

1. Pozastavením VPN přístupu se rozumí proces na straně FN Plzeň, kterým FN Plzeň z dále uvedených důvodů dočasně znemožní zaměstnanci Poskytovatele přístup do vnitřní sítě FN Plzeň.
2. FN Plzeň si vyhrazuje právo pozastavit zaměstnanci Poskytovatele VPN přístup v případě zjištění porušení nebo podezření na nedodržení některého ustanovení této přílohy, příp. při nereagování na validační e-mail nebo při podezření na kybernetickou bezpečnostní událost související s osobou zaměstnance Poskytovatele/Poskytovatele, příp. VPN přístupem (dále jen „Událost“);
3. Po vyhodnocení Události informuje FNP Plzeň Poskytovatele o opětovném umožnění VPN přístupu zaměstnanci Poskytovatele nebo o ukončení VPN přístupu zaměstnanci Poskytovatele, přičemž uvede zdůvodnění svého postupu a své zjištění.
4. Poskytovatel může požádat o pozastavení VPN přístupu zaměstnanci Poskytovatele prostřednictvím zaslání Žádosti dle bodů II. Zřízení VPN přístupu.

Článek 4

Ukončení VPN přístupu

1. Ukončením VPN přístupu se rozumí proces, při kterém je Poskytovateli/zaměstnanci Poskytovatele trvale zablokován přístupu do vnitřní sítě FN Plzeň prostřednictvím VPN FN Plzeň.
2. FN Plzeň ukončí Poskytovateli/ zaměstnanci Poskytovatele VPN přístup:
    a) v případě uplynutí doby, na kterou byl VPN přístup podle Žádosti schválen;
    b) dnem ukončení účinnosti Smlouvy;
    c) na základě žádosti Poskytovatele;
    d) na základě žádosti zaměstnance Poskytovatele;
    e) po příslušném vyhodnocení Události;
    f) na základě žádosti Poskytovatele dle odst. 3., písm. d., e. tohoto článku.
3. Poskytovatel je povinen vždy na e-mail: PIS2@fnplzen.cz a telefonicky na tel.: +420 603 220 976 (FN Plzeň výslovně vyžaduje duplicitní informaci, tedy telefonem a e-mailem), bezodkladně informovat FN Plzeň v případech, když:
    a) došlo k podezření na kompromitaci přihlašovacího hesla k přidělenému uživatelskému jménu zaměstnance Poskytovatele sloužícímu pro VPN přístup;
    b) došlo k podezření na ztrátu/odcizení nebo ke ztrátě/ odcizení koncového zařízení zaměstnanci Poskytovatele, z něhož realizuje VPN přístup;

    bezodkladně žádat FN Plzeň o ukončení VPN přístupu v případech, když:

    c) došlo/dojde k ukončení smluvního vztahu mezi zaměstnancem Poskytovatele a Poskytovatelem;

d) zaměstnanec Poskytovatele se přestal/přestane podílet na plnění závazků Poskytovatele dle Smlouvy;

e) došlo/dojde k ukončení smluvního vztahu mezi Poskytovatelem a jeho poddodavatelem, je-li zaměstnanec Poskytovatele ve smluvním vztahu k tomuto poddodavateli.

Odpovědnost za veškeré činnosti realizované pod přiděleným účtem příslušného zaměstnance Poskytovatele ve vnitřní síti FN Plzeň nese do splnění příslušné povinnosti podle tohoto odstavce Poskytovatel.

1. VPN přístup bude v případech uvedených:

   a) pod písm. a. nebo b. odst. 2. tohoto článku ukončen příslušným dnem;

   b) pod písm. c. nebo d. odst. 2. tohoto článku do 3 pracovních dnů od doručení žádosti o ukončení VPN přístupu, pokud nebude v žádosti o ukončení VPN přístupu požadováno pozdější datum ukončení;

   c) pod písm. e. nebo f. odst. 2. tohoto článku po vyhodnocení Události /po doručení žádosti FN Plzeň.

2. V případě ukončení VPN přístupu dle odst. 2., písm. d., tohoto článku je zaměstnanec Poskytovatele povinen o této skutečnosti neprodleně informovat Poskytovatele; splnění této jeho povinnosti si zajistí Poskytovatel.

Článek 5

Povinnosti Poskytovatele a zaměstnance Poskytovatele

1. Poskytovatel je povinen dodržovat všechna ustanovení této přílohy a zajistit jejich dodržování jednotlivými zaměstnanci Poskytovatele.

2. Poskytovatel je povinen:

   a) prokazatelně seznámit zaměstnance Poskytovatele s právy a povinnostmi vyplývajícími pro něj z této přílohy a prokazatelně zaměstnance Poskytovatele poučit o jeho povinnostech uvedených v této příloze, a to nejpozději v den podání příslušné Žádosti a na vyzvání FN Plzeň tuto skutečnost také FN Plzeň ve lhůtě uvedené v příslušné písemné výzvě, která nebude kratší než 10 pracovních dnů, doložit;

   b) zajistit, aby zaměstnanec Poskytovatele dodržoval povinnosti a postupy vyplývající pro něj z této přílohy;

   c) zajistit, že jsou zaměstnancem Poskytovatele dodržována taková bezpečnostní opatření, která zamezí narušení nebo ohrožení bezpečnosti vnitřní sítě FN Plzeň, informačního systému a informací FN Plzeň.

3. FN Plzeň je oprávněna kontrolovat plnění ustanovení této přílohy na straně Poskytovatele. Poskytovatel je povinen poskytnout FN Plzeň nezbytné podklady, součinnost, případně umožnit kontrolu na místě.

4. Poskytovatel je dále povinen zajistit, aby zaměstnanec Poskytovatele realizoval VPN přístup pouze z koncového zařízení, které:

   a) je chráněno antivirovou a antimalwarovou ochranou a má aktuální virovou databázi;

   b) má instalováno a má aktivní (zapnuto) firewalové řešení operačního systému, příp. HIDS/HIPS (Host Intrusion Detection System/ Host Intrusion Prevention Systém jsou řešení, která umožňují ochránit uživatele, operační systém a data před útoky po síti a před škodlivým kódem);

   c) má instalovány dostupné bezpečnostní záplaty a aktualizace zveřejněné výrobcem operačního systému a aplikací a operační systém je podporovaný výrobcem;

   d) má nastaveno uzamčení koncového zařízení v případě nečinnosti zaměstnance Poskytovatele;

   e) má chráněn přístup do BIOS koncového zařízení;

   f) má šifrován pevný disk koncového zařízení;

g) umožňuje přístup ke koncovému zařízení pouze po zadání přihlašovacích údajů.

5. Povinnosti zaměstnance Poskytovatele:
   a) realizovat přístup do vnitřní sítě FN Plzeň pouze prostřednictvím VPN FN Plzeň;
   b) pro přístup do vnitřní sítě FN Plzeň používat jako přihlašovací heslo unikátní, tj. heslo, které není shodné s jinými hesly používanými zaměstnancem Poskytovatele (kdekoliv);
   c) nesmí sdílet s třetími osobami své přístupové údaje určené pro VPN přístup;
   d) nesmí sdílet VPN připojení s jiným zařízením prostřednictvím sdílení připojení na síťové úrovni;
   e) neukládat své přihlašovací údaje pro VPN přístup do koncového zařízení;
   f) nezasahovat do konfiguračních souborů a nastavení VPN klienta dodaného ze strany FN Plzeň;
   g) ukončit VPN přístup (navázané spojení) v případě, že koncové zařízení nechává bez dozoru;
   h) nepokoušet se narušit bezpečnost vnitřní sítě FN Plzeň;
   i) bezodkladně žádat FN Plzeň prostřednictvím tel.: +420 603 220 976 a e-mailu: pis2@fnplzen.cz (FN Plzeň výslovně vyžaduje duplicitní žádost, tedy telefonem a e-mailem):
      i. zablokování přístupových údajů sloužících k VPN přístupu v případě podezření na kompromitaci/ ztrátu/odcizení koncového zařízení nebo přístupových údajů;
      ii. zablokování přístupových údajů k VPN přístupu v případě zjištění dalších hrozeb narušení bezpečnosti vnitřní sítě FN Plzeň, např. výskyt spywaru.
   j) chránit informace získané při VPN přístupu, a to i tehdy, pokud přímo nesouvisejí s plněním dle Smlouvy, za což nese i osobní odpovědnost;
   k) zachovávat mlčenlivost o všech skutečnostech, se kterými se seznámil v rámci plnění Smlouvy a které nejsou veřejně známé nebo veřejně dostupné;
   l) vzít na vědomí, že FN Plzeň je oprávněna monitorovat přístupy zaměstnance Poskytovatele do informačních systémů a vnitřní sítě FN Plzeň a je oprávněna pozastavit/ukončit zaměstnanci Poskytovatele VPN přístup v případě nesplnění jeho povinností a požadavků uvedených v této příloze;
   m) odpovědět na validační e-mail FN Plzeň nejpozději do 14 kalendářních dnů ode dne, kdy mu byl doručen.

6. Poskytovatel nese plnou odpovědnost za nedodržení povinností kterýmkoli zaměstnancem Poskytovatele daných zaměstnanci Poskytovatele touto přílohou.

Článek 6

Sankce

1. Pokud Poskytovatel nesplní své povinnosti stanovené v Čl. 5., odst. 2., písm. a. této přílohy, tj. že ve lhůtě uvedené v příslušné písemné výzvě nedoloží FN Plzeň příslušné skutečnosti, a to ani přes dodatečnou přes písemnou výzvu FN Plzeň s poskytnutím přiměrné lhůtě k nápravě, je Poskytovatel povinen za každý den prodlení zaplatit FN Plzeň smluvní pokutu ve výši 500 Kč.
2. Za porušení jednotlivých povinností daných touto přílohou Poskytovateli, které Poskytovatel neodstranil ani přes písemnou výzvu FN Plzeň s poskytnutím přiměrné lhůtě k nápravě:
   a) v Čl. 2., odst. 3. této přílohy nebo
   b) v Čl. 4., odst. 3., písm. a. až e. této přílohy nebo
   c) v Čl. 5., odst. 2., písm. a. této přílohy, tj. že zaměstnance Poskytovatele neseznámí s jeho právy a povinnostmi nebo nepoučí zaměstnance Poskytovatele o jeho povinnostech vyplývajících pro zaměstnance Poskytovatele z této přílohy nebo
   d) v Čl. 5., odst. 2., písm. b. nebo c. této přílohy nebo
   e) v Čl. 5 odst. 4. písm. a. až g. této přílohy

je Poskytovatel povinen zaplatit FN Plzeň v každém jednotlivém případě porušení příslušné povinnosti smluvní pokutu ve výši 25 000 Kč, a to i opakovaně.

3. Za porušení jednotlivých povinností daných touto přílohou zaměstnanci Poskytovatele v Čl. 5., odst. 5., písm. a. až m. této přílohy, které Poskytovatel neodstranil ani přes písemnou výzvu FN Plzeň s poskytnutím příměrné lhůtě k nápravě, je Poskytovatel povinen zaplatit FN Plzeň v každém jednotlivém případě porušení příslušné povinnosti smluvní pokutu ve výši 10 000 Kč, a to i opakovaně.
4. Pokud dojde současně k porušení jedné a téže povinnosti uložené touto přílohou Poskytovateli i zaměstnanci Poskytovatele, lze příslušnou sankci uplatnit vůči Poskytovateli pouze 1x; tím není vyloučena možnost opakovaného postihu Poskytovatele, pokud opětovně k porušení jedné a téže povinnosti dojde.
5. Odpovědnost za škodu se řídí ustanovením § 2894 a násl. občanského zákoníku. Sjednáním ani zaplacením smluvní pokuty není dotčeno právo oprávněné smluvní strany na náhradu škody přesahující rozsah uhrazené smluvní pokuty.
6. Za škodu způsobenou porušením povinností stanovených touto přílohou odpovídá Poskytovatel, a to jak za škody způsobené porušením jeho povinností, tak za škody způsobené porušením povinností zaměstnancem Poskytovatele. Zaměstnanec Poskytovatele se pro účely tohoto ustanovení považuje za pomocníka Poskytovatele ve smyslu § 2914 věta první občanského zákoníku.

Článek 7

Závěrečná ustanovení

1. Pokud není v těchto Podmínkách výslovně stanoveno jinak, komunikují Poskytovatel a FN Plzeň ve věci VPN přístupu prostřednictvím pověřených osob uvedených ve Smlouvě.
2. V případě, že v době trvání Smlouvy bude nutné přijmout takové bezpečnostní opatření, které vyvolá potřebu upravit tyto Podmínky, zejména bude-li se jednat o bezpečnostní opatření směřující ke zlepšení systému řízení bezpečnosti informací ve FN Plzeň, řešení kybernetického bezpečnostního incidentu a s tím spojené potřeby minimalizace vzniklého bezpečnostního rizika nebo o povinnost přijmout opatření vydané Národním úřadem pro kybernetickou a informační bezpečnosti dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, zavazují se smluvní strany Smlouvy vyvinout maximální součinnost směřující k uzavření dodatku ke Smlouvě, kterým budou tyto Podmínky odpovídajícím způsobem upraveny.