SMLOUVA O POSKYTOVÁNÍ SERVISNÍ PODPORY

uzavřená ve smyslu ustanovení § 1724 a následujících Zákona č. 89/2012 Sb.,
Občanského zákoníku, v platném znění (dále jen „OZ“)

Článek 1
Smluvní strany

1.1. Dodavatel:
SEFIRA spol. s r.o.
Antala Staška 2027/77, 140 00 Praha 4
IČ: 62907760
DIČ: CZ 62907760
Bankovní spojení: XXX
Číslo účtu: XXX
Zapsaný v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 34572.
Zastoupený: XXX
XXX

1.2. Objednatel:
Česká republika - Státní ústav pro kontrolu léčiv, organizační složka státu
Šrobárova 48, 100 41, Praha 10
IČ: 00023817
bankovní spojení, č.ú.: 623101/0710
Zastoupený: Mgr. Irenou Storovou, MHA, ředitelkou

Článek 2
Předmět smlouvy

2.1. Dodavatel bude poskytovat Objednateli servisní podporu pro Dodavatelem implementovaný produkt OBELISK Seal (dále jen „Systém“).

2.2. Servisní podpora bude poskytována v pracovních dnech v době od 8:00 do 17:00 hodin.

2.3. V rámci servisní podpory budou poskytovány následující servisní služby:

a) garantovaný servisní systém pro hlášení incidentů s garantovanou reakční dobou a dobou vyřešení požadavku dle článku 5.

b) předplacené služby v rozsahu 48 hodin po dobu účinnosti smlouvy zahrnující

- řešení incidentů;
- technické konzultace související s provozem a údržbou Systému;
- změny konfigurace a revize nastavení Systému a
- drobné integrační provozní úpravy (např. připojování oprávněných systémů).

c) servisní práce v místě instalace Systému, pokud je incident nahlášený dle bodu 5.3, není možné jej vyřešit vzdáleně a Objednatel s realizací v místě instalace souhlasí.

2.4. Objednatel v souladu s § 4a odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „ZoKB“) informuje Dodavatele, že systém kvalifikovaného pečetění, jehož součástí je i Systém, je podpůrným systémem systému kritické informační infrastruktury a významných informačních systémů ve smyslu § 2 písm. b) a d) ZoKB a Objednatel je ve smyslu § 2 písm. e) ZoKB správcem tohoto Systému, přičemž Dodavatel bere toto na vědomí. Dodavatel rovněž bere na vědomí, že se po dobu účinnosti této Smlouvy stává provozovatelem Systému ve smyslu § 2 písm. g) ZoKB a dle § 3 písm. e) rovněž osobou, jíž jsou v této souvislosti ZoKB a příslušnými prováděcími předpisy ukládány povinnosti v oblasti kybernetické bezpečnosti. Při plnění této Smlouvy je povinen plnit Bezpečnostní pravidla pro významné dodavatele, které tvoří Přílohu č. 1 této Smlouvy. V případě rozporu mezi ustanovením Smlouvy a ustanovením Přílohy č. 1 je rozhodující ustanovení Smlouvy.

Článek 3
Cena

3.1. Objednatel se zavazuje zaplatit Dodavateli za poskytování servisních služeb dle bodu 2.3 písm. a) a b) této smlouvy cenu ve výši **132 000 Kč bez DPH**, a to za poskytování těchto služeb po celou dobu účinnosti této smlouvy**.**

3.2. Po vyčerpání limitu předplacených služeb dle bodu 2.3 písm. b) této smlouvy bude Objednateli účtována cena 2 225,- Kč bez DPH za každou další započatou hodinu poskytování těchto služeb. O vyčerpání limitu předplacených služeb Dodavatel Objednatele bez prodlení informuje. Dodavatel není oprávněn účtovat Objednateli poskytování služeb dle bodu 2.3 písm. b) této smlouvy nad uvedený limit, pokud Objednatel poskytování služeb nad tento limit předem prokazatelně neschválí. Servisní podpora nad rámec předplacených hodin bude vyúčtována na konci účinnosti smlouvy dle odst. 8.1 této smlouvy, pokud se Dodavatel a Objednatel nedohodnou jinak.

3.3. Servisní práce dle bodu 2.3 písm. c) této smlouvy nejsou čerpány z předplacených hodin a jsou zpoplatněny samostatně:

a) částkou 2 225,- Kč/hod bez DPH a

b) cestovným ve výši 15,- Kč/km bez DPH.

Hodinová sazba dle bodu 3.3 písm. a) se počítá od příjezdu technika na místo instalace do doby jeho odjezdu. Cestovné dle bodu 3.3 písm. b) se počítá na cestu k Objednateli a od Objednatele, pouze však na území hlavního města Prahy.

3.4. Celková cena veškerých služeb dle bodu 2.3 této smlouvy nesmí ve svém souhrnu překročit částku 250 000,- Kč bez DPH. Dodavatel je povinen upozornit Objednatele v případě překročení této částky při objednání služeb dle bodu 3.2 a 3.3.

Článek 4
Platební podmínky

4.1. Úhrada ceny dle bodu 3.1 bude provedena na základě daňového dokladu vystaveného Dodavatelem po nabytí účinnosti této smlouvy.

4.2. Cena servisní podpory nad rámec předplacených hodin dle bodu 3.2 bude vyúčtována samostatnou fakturou, vystavenou po pozbytí účinnosti smlouvy dle odst. 8.1.

4.3. Servisní práce v místě instalace Systému budou vyúčtovány samostatnou fakturou po uskutečnění výjezdu a dokončení servisních prací.

4.4. Daňový doklad bude obsahovat veškeré náležitosti požadované platnými právními předpisy, zejména náležitosti stanovené v § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění.

4.5. Lhůta splatnosti faktury činí 30 kalendářních dnů ode dne jejího doručení Objednateli.

4.6. Nebude-li daňový doklad obsahovat stanovené náležitosti nebo v něm budou uvedeny nesprávné údaje, je Objednatel oprávněn jej vrátit ve lhůtě splatnosti zpět Dodavateli s uvedením, resp. vytčením chybějících náležitostí nebo nesprávných údajů. Dodavatel je povinen podle povahy závad fakturu opravit nebo nově vyhotovit. Oprávněným vrácením faktury přestává běžet původní lhůta splatnosti. Nová lhůta splatnosti běží znovu ode dne doručení opravené nebo nově vyhotovené faktury.

4.7. Dodavatel je oprávněn po Objednateli požadovat smluvní pokutu za úhradu faktury po splatnosti ve výši 0,05 % denně z částky, s jejímž zaplacením je Objednatel v prodlení.

4.8. Smluvní pokuta dle bodu 4.7 a 5.8 této smlouvy je splatná do deseti (10) pracovních dnů po doručení oznámení o uplatnění smluvní pokuty oprávněnou Smluvní stranou. Oznámení o uplatnění smluvní pokuty bude obsahovat popis a časové určení události, která v souladu s touto Smlouvou zakládá právo účtovat smluvní pokutu.

Článek 5
Podmínky poskytování servisní podpory

5.1. Místem plnění je místo instalace Systému, kterým se rozumí sídlo Objednatele na adrese Šrobárova 48, 100 41, Praha 10.

5.2. Incidentem se rozumí okolnosti bránící plynulému provozu podporovaného Systému. Jejich kategorizace probíhá dle následujících podmínek:

Úroveň hlášení		**Popis**
Vysoká	„Incident A“	Standardní firemní procesy Objednatele jsou vážně ovlivněny a nezbytné úlohy nemohou být plněny. Některé nebo všechny systémy podporující hlavní firemní procesy selhaly a jsou zcela nefunkční nebo je jejich funkčnost omezena tak, že je kritickým způsobem ovlivněna informační podpora činnosti Objednatele.
Střední	„Incident B“	Jsou dotčeny firemní procesy Objednatele v míře způsobující ztěžování výkonu konkrétní činnosti. Podporované činnosti jsou výrazně ovlivněny z důvodu selhání nebo omezení některé ze systémových funkcí podporující důležité procesy. V případě současného výskytu více vad kategorie B může nastat situace, kdy vzájemné působení těchto vad způsobí kumulaci negativního dopadu na firemní procesy, pak budou i jednotlivé vady způsobující tuto kumulaci hodnoceny kategorií A.
Nízká	„Incident C“	Stav služby, kdy nejsou ohroženy hlavní funkce Systému. Po dobu výpadku lze nahradit nefunkční část náhradním řešením.

5.3. Incident je považovaný ze strany Objednatele za oznámený v případě, že jsou splněny následující podmínky:

- je věcně popsaný,
- je navržena jeho klasifikace a
- je zadaný do servisního systému dle bodu 2.3 písm. a) přes jeho uživatelské rozhraní (nebo v případě nemožnosti zadání do servisního systému e-mailem).
- Jedná-li se o incident úrovně A, byl zároveň nahlášen telefonicky.

5.4. Za čas oznámení se považuje čas zanesení požadavku do servisního systému u incidentu úrovně B a C (v případě zaslání požadavku e-mailem v době nefunkčnosti servisního systému se za čas oznámení považuje okamžik potvrzení telefonickým nahlášením), u incidentu úrovně A čas nahlášení telefonicky.

5.5. Garantovaná reakční doba (potvrzení přijetí požadavku s informací o zahájení řešení incidentu) a garantovaná doba vyřešení incidentu je uvedena v tabulce níže:

Úroveň hlášení		Reakční doba	Doba vyřešení
vysoká	„Incident A“	1 hodina	NBD
střední	„Incident B“	4 hodiny	NBD+1
nízká	„Incident C“	NBD	NBD+5

BD (Business Day) - pracovní den dle českého kalendáře v čase mezi 8:00 až 17:00
NBD (Next Business Day) – následující pracovní den
NBD+x (Next Business Day + x BD) – x-tý pracovní den po NBD

5.6. Reakční doby se počítají v pracovních dnech v čase od 8:00 do 17:00 hodin od času oznámení incidentu.

5.7. Doba vyřešení se počítá od doby reakce Dodavatele na nahlášený incident.

5.8. V případě prodlení Dodavatele s vyřešením požadavku v garantované době dle bodu 5.5 této smlouvy se Dodavatel zavazuje zaplatit Objednateli smluvní pokutu ve výši 1 000,- Kč bez DPH za každý započatý den prodlení. V případě prodlení Dodavatele s převzetím oznámení incidentu v garantované reakční době dle bodu 5.5 této smlouvy se Dodavatel zavazuje zaplatit Objednateli smluvní pokutu ve výši 1 000,- Kč bez DPH za každou započatou hodinu prodlení.

5.9. Nevyčerpá-li Objednatel předplacené hodiny servisní podpory definované v bodě 2.3 písm. b) za dobu účinnosti této smlouvy, pak nárok na jejich vyčerpání propadá.

5.10. Dodavatel se zavazuje, že jeho pracovníci budou při plnění této smlouvy v objektech Objednatele dodržovat všechny všeobecně závazné předpisy vztahující se k vykonávání činností dle této smlouvy, zejména předpisy související s bezpečností práce a protipožární bezpečností, interní předpisy Objednatele, zejména předpisy o vstupu do objektů Objednatele a o zajištění bezpečnosti systémů Objednatele. Dále se Dodavatele zavazuje, že jeho pracovníci se budou při vykonávání činností dle této smlouvy řídit organizačními pokyny oprávněných pracovníků Objednatele.

5.11. Objednatel se zavazuje zajistit pro pracovníky Dodavatele součinnost v pracovní dny od 8:00 do 17:00 hodin v rozsahu dostupnosti proškolených pracovníků Objednatele v místě instalace pro vzájemnou komunikaci a zásahy na Systému. Po dobu, po kterou není poskytována požadovaná součinnost, kterou lze od Objednatele rozumně očekávat, není Dodavatel v prodlení s vyřešením nahlášeného incidentu.

Článek 6
Oprávněné osoby, komunikace

6.1. Kontaktní údaje Dodavatele pro oznamování incidentů a příjem požadavků:

servisní systém pro hlášení incidentů: https://servicedesk.sefira.cz/
e-mail: XXX
telefon: XXX

6.2. Oprávněnými pracovníky Objednatele jsou následující osoby:
XXX
XXX
XXX
XXX

6.3. Smluvní strany jsou oprávněny jednostranně změnit oprávněné osoby, resp. kontaktní údaje, jsou však povinny na takovou změnu druhou stranu předem písemně upozornit.

Článek 7
Ochrana obchodního tajemství a důvěrných informací

7.1. Dodavatel se zavazuje zachovávat mlčenlivost o Důvěrných informacích, které se dozví v souvislosti s plněním povinností plynoucích z této Smlouvy, zajistit Důvěrné informace tak, aby nedošlo k jejich prozrazení Třetím osobám, nevyužívat je ve prospěch svůj ani Třetích stran, nezpřístupnit nebo neumožnit jejich zpřístupnění Třetím stranám bez předchozího písemného souhlasu Objednatele.

7.2. Povinnost zachovávat mlčenlivost v rozsahu tohoto článku Smlouvy trvá neomezeně a Dodavatel se zavazuje ji dodržovat i po skončení této Smlouvy.

Článek 8
Trvání smlouvy

8.1. Tato smlouva se uzavírá na dobu 6 měsíců od nabytí účinnosti této smlouvy.

8.2. Smlouvu lze ukončit

a) písemnou dohodou smluvních stran;

b) výpovědí s výpovědní lhůtou 3 měsíce, jejímž uplynutím povinnost Dodavatele poskytovat Objednateli servisní podporu zaniká; pokud výpověď podal Dodavatel, zavazuje se Dodavatel vrátit Objednateli částku odpovídající nevyčerpaným předplaceným hodinám servisní podpory; pokud výpověď podal Objednatel, pak Dodavatel částku odpovídající nevyčerpaným předplaceným hodinám servisní podpory vracet nemusí;

c) odstoupením od smlouvy v případech podstatného porušení smlouvy, přičemž odstoupení od smlouvy musí být písemné a nabývá účinnosti dnem doručení druhé smluvní straně;

Článek 9
Podstatné porušení smlouvy

9.1. Podstatným porušením smlouvy Objednatelem je prodlení Objednatele s úhradou faktury po dobu delší než 30 dnů.

9.2. Podstatným porušením smlouvy Dodavatelem je opakované prodlení s vyřešením požadavku v garantované době dle bodu 5.5 této smlouvy delší než 5 pracovních dní nebo porušení povinnosti mlčenlivosti stanovené v článku 7.

Článek 10
Závěrečná ustanovení

10.1. Tato smlouva se vyhotovuje ve 2 vyhotoveních s platností originálu, přičemž každá ze smluvních stran obdrží 1 vyhotovení.

10.2. Nedílnou součástí této smlouvy je:

Příloha č. 1 – Bezpečnostní pravidla pro významné dodavatele

Příloha č. 2 – Formulář žádosti o přístup / ukončení přístupu do informačního systému Objednatele

10.3. Tuto smlouvu lze upravovat pouze dohodou smluvních stran písemnými v řadě číslovanými dodatky, jež budou podepsány zmocněnými zástupci obou smluvních stran.

10.4. Ve všech případech, které neřeší ujednání obsažená v této smlouvě, platí příslušná ustanovení OZ, případně dalších předpisů platného práva České republiky.

10.5. Dodavatel bere na vědomí povinnost zveřejnit smlouvu v registru smluv (dále jen „registr smluv“) v souladu se zákonem č. 340/2015 Sb., o registru smluv, a podpisem této smlouvy vyslovuje souhlas se zveřejněním všech údajů uvedených ve smlouvě Objednatelem v registru smluv zřízeném uvedeným zákonem, vyjma osobních údajů. Dodavatel výslovně prohlašuje, že žádný údaj uvedený v této smlouvě a jejích přílohách není obchodním tajemstvím ve smyslu § 504 OZ.

10.6. Smlouva nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti dnem uveřejnění této smlouvy v registru smluv.

10.7. Stane-li se některé ustanovení smlouvy neplatným nebo neúčinným, nedotýká se to ostatních ustanovení této smlouvy, která zůstávají platná a účinná. Smluvní strany se zavazují dodatkem k této smlouvě nahradit ustanovení neplatné či neúčinné novým ustanovením platným nebo účinným, které nejlépe odpovídá původně zamýšlenému účelu ustanovení neplatného nebo neúčinného. Do té doby platí odpovídající úprava obecně závazných právních předpisů České republiky.

10.8. Smluvní strany po přečtení smlouvy prohlašují, že souhlasí s jejím obsahem bez výhrad, že tato byla sepsána na základě pravdivých údajů, jejich pravé a svobodné vůle a nebyla ujednána v tísni, ani za jinak jednostranně nevýhodných podmínek a zároveň prohlašují, že jim nejsou známy žádné skutečnosti, které by bránily řádnému uzavření smlouvy a jejímu plnění.

Na důkaz toho připojují své vlastnoruční podpisy.

V Praze dne 19.4.2023

Za Objednatele

……
Mgr. Irena Storová, MHA, ředitelka
Státního ústavu pro kontrolu léčiv

V Praze dne 4.4.2023

Za Dodavatele

……
XXX

……
XXX

BEZPEČNOSTNÍ PRAVIDLA PRO VÝZNAMNÉ DODAVATELE dle ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI (č. 181/2014 Sb.) a VYHLÁŠKY č. 82/2018 Sb.

1 PERSONÁLNÍ BEZPEČNOST

1.1 Smluvní partner Státního ústavu pro kontrolu léčiv (dále jen „SÚKL“) a jeho případní subdodavatelé (smluvní partner a subdodavatelé dále jen souhrnně „dodavatel“) mají povinnost ve svých interních procesech realizovat tato opatření:

a) mít stanoven vlastní plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí a který obsahuje formu, obsah a rozsah:

i. poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice;
ii. potřebných teoretických i praktických školení uživatelů, administrátorů a osob zastávajících bezpečnostní role, nebo zajišťujících podporu provozu informačního systému SÚKL;

b) mít určeny osoby odpovědné za realizaci jednotlivých činností, které jsou v plánu uvedeny;

c) v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení;

d) pro osoby zastávající bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat pravidelná odborná školení, přičemž vychází z aktuálních potřeb v oblasti kybernetické bezpečnosti;

e) v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní;

f) zajišťovat kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role;

g) v případě ukončení smluvního vztahu s administrátory a osobami podílejících se na podpoře vývoje či provozu systému SÚKL či jakékoliv jeho infrastrukturní části, zajišťovat předání odpovědností, zrušení jejich přístupových účtů a informovat SÚKL o této skutečnosti;

h) stanovit interní pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany administrátorů a osob zastávajících bezpečnostní role;

i) vést o provedených školeních přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.

1.2 SÚKL si vyhrazuje právo vést záznamy a prověřovat činnosti dodavatele, vést záznamy o incidentech a nestandardních činnostech zaměstnanců a dalších osob působících ve prospěch dodavatele (dále jen „zaměstnanci dodavatele“). Na základě těchto záznamů má oprávnění vyhodnocovat důvěryhodnost a spolehlivost zaměstnanců dodavatele, zejména při situacích vzniklých bezpečnostních incidentů. V případě identifikovaného rizika oznámí SÚKL nesoulad dodavateli a obě strany vejdou v jednání pro řešení této situace.

1.3 Kvalifikace zaměstnanců dodavatele musí odpovídat vykonávané pracovní pozici (vykonávané práci a úrovni zabezpečení).

2 FYZICKÁ BEZPEČNOST, POŽÁRNÍ OCHRANA A BOZP

2.1 Dodavatel jako zaměstnavatel při provádění prací při plnění smlouvy odpovídá za dodržování předpisů BOZP a PO svými zaměstnanci v prostorách SÚKL, popř. dalšími fyzickými osobami

vykonávajícími práci v jeho prospěch a odpovídá za dodržování podmínek vstupu osob a vjezdu vozidel do areálů, objektů a na pozemky SÚKL a bezpečnostního režimu pro ně stanoveného.

3 BEZPEČNOSTNÍ POVĚDOMÍ

3.1 Každý zaměstnanec dodavatele musí být prokazatelně proškolen a mít znalosti příslušných interních předpisů SÚKL souvisejících s předmětem plnění smlouvy. Za proškolení zaměstnanců dodavatele (v roli provozovatele) a za jejich prokazatelné seznámení s požadavky smlouvy a jejích příloh odpovídá dodavatel.

4 IDENTIFIKACE

4.1 Každý zaměstnanec dodavatele podílející se na plnění smlouvy výpočetními prostředky dodavatele, musí mít v rámci své ICT infrastruktury evidován a veden svůj vlastní jedinečný uživatelský účet, kterému jsou v jednotlivých určených systémech, modulech nebo aplikacích přiřazeny specifické role. Každý zaměstnanec dodavatele musí být veden s platnými identifikačními a aktuálními kontaktními údaji. Na technická zařízení, se kterými zaměstnanci dodavatele přistupují do vymezených částí vnitřní infrastruktury SÚKL, se ze strany SÚKL pohlíží jako na BYOD a pro jejich konfiguraci se vyžaduje dodržování minima dle vnitřního předpisu SÚKL S-069, který je dodavateli předán.

4.2 Každý zaměstnanec dodavatele, pokud přistupuje k interním systémům SÚKL, má u SÚKL veden a evidován jedinečný uživatelský účet, kterému jsou v jednotlivých systémech, modulech nebo aplikacích přiřazeny specifické role související výhradně s plněním předmětu smlouvy.

5 AUTENTIZACE

5.1 Podmínky pro autentizaci při využití ICT infrastruktury SÚKL:

a) k jednoznačné identifikaci privilegovaných uživatelů určených systémů se preferovaně využívá vícefaktorová autentizace;

b) ověření heslem - pokud není možné použít jednoznačnou identifikaci privilegovaných uživatelů více faktory, je použita autentizace heslem o minimální délce 17 znaků, kdy mezi znaky musí být minimálně jedno velké písmeno, jedno malé písmeno, jedna číslice a jeden metaznak z možností: #, $, &, %, !, ?, +, - Heslo musí být měněno nejpozději po 18 měsících, případně v kratším intervalu vyžadovaném aktuálně nastavenou politikou hesel, a nesmí se následně zopakovat v následných 12ti změnách.

5.2 Pro vzdálený přístup zaměstnanců dodavatele předkládá dodavatel podklady pro vyplnění žádosti o vzdálený přístup, podle které jsou poté nastavena oprávnění. Žádost podepisuje oprávněná osoba dodavatele jednat ve věcech plnění smlouvy.

5.3 Dodavatel odpovídá za činnosti svých zaměstnanců, popřípadě dalších fyzických osob vykonávajících práci v jeho prospěch, které musí být v souladu s pravidly, předanými ze strany SÚKL. Veškeré škody, které vzniknou porušením těchto pravidel zaměstnanci dodavatele nebo dalšími fyzickými osobami vykonávajícími práci v jeho prospěch, jdou k tíži dodavatele, který je povinen tyto škody v plném rozsahu SÚKL nahradit.

6 AUTORIZACE

6.1 Zaměstnanci dodavatele jsou povinni v ICT infrastruktuře SÚKL využívat privilegovaná oprávnění jen v přiměřené míře a jen po dobu nezbytně nutnou pro vykonání činností v souladu s plněním předmětu smlouvy. Uživatelé ani administrátoři nesmějí používat účty s privilegovanými oprávněními

pro běžnou práci nesouvisející se správou určeného systému a v žádném případě nesmí umožnit pracovat pod tímto účtem jiným osobám.

6.2 Zaměstnanci dodavatele jsou informováni SÚKL, ke kterým chráněným informacím SÚKL mají při plnění smlouvy přístup a jak s nimi mohou nakládat. Tyto informace vyplývají ze smlouvy a dodavatel je oprávněn a povinen své zaměstnance s příslušnými částmi smlouvy prokazatelně seznámit. Jakékoliv manipulace a další operace s chráněnými informacemi SÚKL, které nebyly výslovně v instrukcích uvedeny, nemá dodavatel povoleny.

7 KONCOVÁ PRACOVNÍ STANICE

7.1 Pro přístup k systémům SÚKL jsou standardně použity vlastní prostředky dodavatele (HW, SW). Dodavatel odpovídá za to, že nejsou používány v rozporu s licenčními podmínkami produktů.

7.2 Přístup výpočetní techniky dodavatele (PC, notebooky) k chráněným interním informacím a k informačním a telekomunikačním systémům je podmíněn schválením příslušného pracoviště SÚKL a odpovědnou osobou systému.

7.3 Pracovní stanice dodavatele přistupující prostřednictvím VPN musí splňovat podmínky uvedené pro používání BYOD v interní směrnici SÚKL S-069.

8 UŽÍVÁNÍ KRYPTOGRAFICKÝCH PROSTŘEDKŮ

8.1 Je-li v rámci předmětu plnění vyžadováno použití kryptografických prostředků, technické podmínky jsou následující:

a) užití pouze kryptografických prostředků podle doporučení vydávaných a aktualizovaných NÚKIB

b) šifrování pomocí digitálních certifikátů vydaných obecně uznávanou CA nebo CA, které explicitně důvěřují obě strany;

c) pro webové servery prezentující data pocházející z určených informačních systémů mimo samotný systém používat HTTPS protokol;

d) pro webové servery prezentující data pocházející z určených systémů pro uživatele mimo SÚKL se používá certifikát obecně uznávané certifikační autority.

9 MONITORING

9.1 Přístup zaměstnanců dodavatele k vybraným chráněným interním informacím a k informačním a komunikačním systémům SÚKL může být nepřetržitě zaznamenáván, monitorován a vyhodnocován. Události v systémech jsou SÚKL zaznamenávány do logů.

9.2 Dodavatel je povinen průběžně monitorovat v rámci své ICT infrastruktury zveřejněné a známé bezpečnostní chyby, které mohou ovlivnit hladký a bezpečný provoz systémů souvisejících s jím poskytovanými službami. Jedná se například o zranitelnosti v operačních systémech, software třetích stran, webové komponenty atd.

9.3 V souladu s příslušnými ustanoveními smlouvy je dodavatel povinen neprodleně po zjištění hlásit SÚKL každý nastalý bezpečnostní incident.

10 OCHRANA MÉDIÍ

10.1 Uložení chráněných informací SÚKL na přenosná média a případný transport médií mimo prostory SÚKL podléhá jeho schválení.

10.2 V případě ukládání chráněných informací SÚKL na přenosná média má dodavatel povinnost, pokud je to technicky možné, ukládat, případně vyžadovat uložení těchto dat v šifrované podobě a vést evidenci těchto médií.

10.3 Dodavatel je povinen zajistit likvidaci operativních dat obsahujících chráněné informace SÚKL ihned po pominutí účelu jejich zpracování a/nebo uložení způsobem dle právních předpisů či metodik vydaných NÚKIB, případně ÚOOÚ. Po likvidaci dat na elektronickém médiu nesmí být možné informaci obnovit. O provedení likvidace dat musí dodavatel vést protokol.

11 BEZPEČNOSTNÍ UDÁLOSTI / INCIDENTY

11.1 Dodavatel má za povinnost hlásit veškerá podezření na kybernetické bezpečnostní události:

a) odpovědné osobě SÚKL (osoba oprávněná jednat ve věcech plnění smlouvy a manager kybernetické bezpečnosti). Ohlášení provede mailem (případně telefonicky) v termínu bezprostředně (bez prodlení) po zjištění kybernetické bezpečnostní události / incidentu.

b) v ohlášení uvede:

i. datum a čas zjištění;
ii. povahu události / incidentu;
iii. zdroje události;
iv. cíle / oběti události;
v. okamžité i potencionální dopady;
vi. přijatá či navrhovaná opatření k omezení dopadů, případně eliminaci opakování.

12 AUDIT DODAVATELE (PRAVIDLA ZÁKAZNICKÉHO AUDITU)

12.1 OPRÁVNĚNÍ K PROVEDENÍ AUDITU DODAVATELE

a) SÚKL si v souladu s ustanovením smlouvy vyhrazuje právo provádět audity dodavatele.

b) SÚKL s dostatečným předstihem alespoň 5 pracovních dnů oznámí dodavateli záměr na provedení auditu. Obě strany si dohodnou obsah, potřebnou součinnost a časový plán auditu s tím, že SÚKL se zavazuje postupovat tak, aby nenarušil provozní potřeby dodavatele.

c) SÚKL si vyhrazuje právo v případě závažných důvodů (např. podezření na rizikové chování dodavatele) v souvislosti s plněním smlouvy provést neohlášený audit u dodavatele s přihlédnutím k provozní situaci dodavatele.

d) Dokumentace auditů prováděných SÚKL tvoří pro každý audit:

i. oznámení o auditu a plán auditu;
ii. dotazník k auditu (seznam otázek auditora, pokud auditor uzná za vhodné);
iii. zpráva z auditu;
iv. písemné, fotografické nebo jiné záznamy provozu, postupů nebo zařízení, které souvisí s auditem (pokud je nezbytné pro dokumentování nálezů);
v. záznam o zjištění (nápravných opatřeních a následné kontrole).

f) Auditovaná strana (dodavatel) obdrží k vyjádření závěrečnou zprávu auditu obsahující případná zjištění:

i. dodavatel navrhne na základě zjištění uvedených v závěrečné auditní zprávě návrh opatření a termíny řešení a předá jejich seznam SÚKL k odsouhlasení;
ii. SÚKL potvrdí souhlas s navrženými opatřeními. Souhlas vydává osoba oprávněná jednat ve věcech smlouvy.

12.2 NÁPRAVNÁ OPATŘENÍ

a) Auditovaná strana (dodavatel) má za povinnost v určeném čase zajistit realizaci dohodnutých nápravných opatření;

b) Zprávu o realizovaných opatřeních dodavatel oznamuje a předává SÚKL cestou člena jeho auditního týmu.

13 PODMÍNKY PŘI UKONČENÍ SMLOUVY

13.1 V případě ukončení smluvního vztahu musí být ukončeny veškeré přístupy dodavatele a jeho zaměstnanců k aktivům společnosti (VPN, systémy, informace) nejpozději k termínu ukončení smluvního vztahu.

13.2 Pokud byla zaměstnancům dodavatele poskytnuta aktiva SÚKL, musí být tato aktiva vrácena nejpozději k termínu ukončení smluvního vztahu.

13.3 Pokud byla dodavateli poskytnuta informační aktiva (data) SÚKL, musí být nejpozději k termínu ukončení smluvního vztahu vrácena a beze zbytku smazána způsobem určeným v právních předpisech o kybernetické bezpečnosti, či metodice NÚKIB, resp. ÚOOÚ, ze všech systémů dodavatele a nosičů dodavatele taková aktiva obsahujících. O smazání či předání takových aktiv musí být vypracován protokol, který je předán SÚKL.

13.4 V případě předčasného ukončení smluvního vztahu jiným způsobem než splněním závazku (např. výpovědí, odstoupením od smlouvy, dohodou o ukončení smlouvy apod.), mohou být přístupy dodavatele, pokud je to nutné, ze strany SÚKL ukončeny před uplynutím doby trvání smluvního vztahu.

SÚKL STÁTNÍ ÚSTAV PRO KONTROLU LÉČIV Šrobárova 48 100 41 Praha 10 Telefon: +420 272 185 111 Fax: +420 271 732 377 E-mail: posta@sukl.cz Web: www.sukl.cz

Příloha č. 2 – Formulář žádosti o přístup / ukončení přístupu do informačního systému Objednatele

…… IČ: …… (dále jen „žadatel“) žádá o zavedení přidělení přístupu / ukončení přístupu na servery SÚKL *(nehodící se škrtněte)*

pro své následující zaměstnance :

Jméno a příjmení	Telefonní číslo	E-mailová adresa

Předmětem žádosti jsou přístupová oprávnění na servery:

Název serveru		IP adresa

za účelem plnění smlouvy ……. ze dne ……. /objednávky ……. ze dne ……. .

Přístupy k serverům lze použít pouze za uvedeným účelem. Žadatel a jeho zaměstnanci jsou povinni přístupová oprávnění chránit proti neoprávněnému použití či jakémukoliv zneužití. Současně se zavazují, že informace, se kterými se seznámí, použijí pouze k účelu, pro který jim byl přístup povolen, a nebudou je dále šířit.

Žadatel zpřístupní přístupová oprávnění pouze svým výše uvedeným zaměstnancům pověřeným prováděním činností v rámci plnění výše uvedené smlouvy / objednávky. Žadatel se zavazuje, že bude přistupovat pouze k serverům, o které požádal a pokud skončí potřeba přístupu, neprodleně o tomto SÚKL informuje. Žadatel je povinen SÚKL neprodleně informovat o skutečnosti, že zaměstnanec, kterému bylo přiděleno přístupové oprávnění, přestal pro žadatele vykonávat činnosti, pro něž mu byla přístupová oprávnění udělena. Převod přístupového oprávnění na jiného zaměstnance žadatele podléhá předchozímu schválení ze strany SÚKL, o nějž je žadatel povinen požádat novou žádostí.

Neoprávněné použití přístupových oprávnění žadatelem či jeho zaměstnancem je považováno za porušení uděleného povolení, které zakládá plnou odpovědnost za takové porušení dle platných právních předpisů.

Žadatel i jeho zaměstnanci přistupující k serverům SÚKL se zavazují k dodržování veškerých povinností vyžadovaných při ochraně osobních údajů příslušnými platnými právními předpisy, zejména Obecným Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27.dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) a zákonem č. 127/2005 Sb. o elektronických komunikacích a neumožní žádné jiné osobě získat a zpracovávat takovéto údaje. V případě porušení ochrany osobních údajů je žadatel povinen neprodleně informovat písemně SÚKL odesláním informace o incidentu na adresu posta@sukl.cz. Podpisem této žádosti žadatel osvědčuje, že jeho zaměstnanci jsou plně obeznámeni s povinnostmi stanovenými v právních předpisech dle předchozí věty a že získal souhlas uvedených zaměstnanců k tomu, aby jejich zde uvedené osobní údaje byly předány SÚKL a jím evidovány/zpracovávány pro účely plnění smlouvy/objednávky.

Žadatel odpovídá SÚKL za veškeré škody, způsobené porušením povinností stanovených v této žádosti či v platných právních předpisech ze strany žadatele či jeho zaměstnance. Každou takovou škodu je žadatel povinen nahradit SÚKL v plné výši.

Datum: ……. ……

Podpis

Schválil manažer bezpečnosti informací SÚKL

Datum: ……. ……

Podpis