Janiga Labs, s.r.o.
Moravanů 68
169 00 PRAHA 6
IČO: 63 99 01 48, DIČ: 006-63990148

PO 263/Kr/05

Smlouva o poskytnutí a servisu informačního systému mikrobiologie

č. 177/2005

I.
Smluvní strany

1. Všeobecná fakultní nemocnice v Praze
se sídlem : U nemocnice 2
128 08 Praha 2
IČO : 00064165
bankovní spojení : CZ00064165
číslo účtu : 24035-021/0100
zastoupená ředitelem nemocnice panem **MUDr. Pavlem Horákem, CSc., MBA**
(dále jen "**objednatel** ")

a

2. Janiga Labs, s.r.o.
se sídlem : Moravanů 68
169 00 Praha 6
bankovní spojení: [redacted]
IČO : [redacted]
DIČ : [redacted]
zapsáno v obchodním rejstříku Městského soudu v Praze v oddílu C vložka 38795.
zastoupená jednatelem společnosti panem **RNDr. Ladislavem Janigou, CSc., PhD**
(dále jen "**dodavatel**")

II.
Vymezení pojmů

1. Objednatelem a uživatelem je podle této smlouvy Všeobecná fakultní nemocnice tak, jak je uvedeno v záhlaví této smlouvy.
2. Dodavatelem je podle této smlouvy Janiga Labs, s.r.o., tak, jak je uvedeno v záhlaví této smlouvy.

III.
Předmět plnění

1. Předmětem plnění této smlouvy je poskytnutí licencí a zabezpečení servisu k informačnímu systému, jehož komponenty jsou jmenovitě následující:
   A. Laboratorní systém pro mikrobiologii, serologii a virologii
   B. Agenda nemocničních a komunitních infekcí
   C. Konzultační systém pro antibiotickou terapii
   D. Agenda spotřeby antibiotik
   E. Agenda evidence kmenů
   F. Žádankový systém pro vázaná antibiotika
   G. Auditovací systém
2. Taxativní výčet poskytnutých komponent je uveden v Příloze 1 této Smlouvy, která je její nedílnou součástí. Komponenty jsou poskytnuty včetně specifické konfigurace, implementace do místního prostředí informačních systémů a zaškolení personálu. Rozhraním na celonemocniční informační systém se rozumí výměna vyúčtovacích dat, žádanek, výsledků a statistik. Technická implementace rozhraní bude realizována Dodavatelem podle konkrétní specifikace Objednatele, výměna dat v obou směrech bude implementována JDBC konektivitou nebo některým z protokolů nfs, smb, ssh či ftp a to formou textových nebo XML dokumentů.
3. Parametry a promptnost servisu. Reakční doba ze strany Dodavatele se pro zahájení servisního zásahu stanovuje na 4 hodiny od nahlášení požadavku. Zásah administrátora si vyžádá uživatel telefonicky v pracovních dnech mezi 9:00 a 16:00 na číslech [redacted] fax) a mimo pracovní dny na číslech [redacted] Dodavatel se zavazuje zahájit záruční i nezáruční opravy do čtyř hodin od okamžiku nahlášení závady. Dojde-li ke změně telefonních čísel zhotovitele, bude o tom objednatel neprodleně informován.

4. Servis se nevztahuje na závady způsobené zejména neodbornou či nevhodnou manipulací s technickým vybavením, úmyslným poškozením, krádeží, objednatelem neautorizovanými zásahy, zásahem vyšší moci nebo provozováním systému v nevyhovujících podmínkách. Servis se také nevztahuje na technické závady a na závady operačního systému pracovních stanic či síťové infrastruktury Objednatele. Dodavatel se nicméně zavazuje k poskytnutí nezbytných informací o vhodné konfiguraci počítačů v případě, že objednatel bude nucen počítače po odstranění technické závady rekonfigurovat a znovu zprovoznit.
5. Servis se výslovně vztahuje na tyto činnosti:
    a. Poskytování nových verzí systému i provozní infrastruktury včetně instalace
    b. Pomoc při akceptování konfiguračních souborů, programovatelných formulářů a dalších komponent systému vznikajících průběžně v referenční verzi systému.
    c. Údržba provozního serveru systému, aktualizace systémových komponent.
    d. Průběžná správa systému a proaktivní detekce provozních problémů.
    e. Konzultace nebo vyžádané úpravy konfiguračních dat a programových skriptů v rozsahu do dvou hodin měsíčně.

IV.
Dohoda o ceně a způsob platby

1. Cena za servis systému ve shodě s článkem III je stanovena dohodou smluvních stran ve výši 604,440,-- Kč bez DPH ročně, a to počínaje 1.5.2005. Cena bude zatížena DPH v aktuálně platné sazbě. Cena servisu bude upravena každý rok v dubnu oficiálním indexem spotřebitelských cen vyhlášeným ČNB k 31. březnu, a to formou dodatku k této smlouvě. Datum podepsání dodatku nemá odkladný účinek aktualizované fakturace.
2. Fakturace proběhne vždy k 1.červenci daného roku s tím, že splatnost faktur je 120 dní.

V.
Místo plnění, závazky objednatele, uživatele a zhotovitele

1. Místo plnění je shodné se sídlem objednatele.
2. Objednatel se zavazuje zabezpečit fyzický přístup k systému zhotoviteli pro potřeby servisu.
3. Vzdálený datový přístup bude zajištěn prostřednictvím bezpečného kanálu přes veřejnou datovou síť Internet.
4. Objednatel jmenuje odpovědným pracovníkem ve věci koordinace vyžádaného servisu systému prim. MUDr. A.Jedličkovou s oprávněním schválit a převzít servisní zásahy.

VI.
Platnost smlouvy

1. Tato smlouva nabývá platnosti i účinnosti dnem jejího podpisu oběma stranami. Smlouva se uzavírá na dobu tří let s výpovědní lhůtou 12 měsíců pro obě strany.
2. Nebude-li smlouva písemně vypovězena ani jednou ze smluvních stran alespoň 12 měsíců před předpokládaným datem ukončení smlouvy, prodlužuje se platnost implicitně vždy o dalších 12 měsíců.
3. Platnost této smlouvy může být také ukončena po vzájemné písemné dohodě smluvních stran.
4. Prodloužení platnosti smlouvy je možné vzájemnou písemnou dohodou.

VIII.
Závěrečná ustanovení

1. Změny a doplňky této smlouvy jsou přípustné pouze v písemné formě na základě dohody obou stran.
2. Smluvní strany se dohodly, že jejich závazkový vztah založený touto smlouvou se bude řídit zákonem č. 513/1991 Sb., obchodním zákoníkem, v platném znění.
3. Pokud není v této smlouvě sjednáno jinak, řídí se práva a povinnosti smluvních stran příslušnými ustanoveními obchodního zákoníku.
4. Smlouva je vyhotovena ve 4 stejnopisech, z nichž každá strana obdrží po 2 exemplářích.
5. Obě smluvní strany prohlašují, že tuto smlouvu uzavřely na základě vzájemné dohody podle své pravé a svobodné vůle. Toto stvrzují svým vlastnoručním podpisem.

V Praze - 4 IV 05

[redacted]

za [redacted]

[redacted] s, s.r.o.
[redacted] ů 68
[redacted] AHA 6
IČO: 63 99 01 48, DIČ: 006-63990148

C.Konzultační systém pro antibiotickou terapii

- Provozní infrastruktura – identická se sub A.
- Speciální software ve verzi 2005
  - Agenda konzultací
  - Optimalizace léčby
  - Statistický modul
  - Integrace s ostatními mikrobiologickými aplikacemi
  - Agenda antiobiotických přípravků

D.Agenda spotřeby antibiotik

- Provozní infrastruktura – identická se sub A.
- Speciální software ve verzi 2003, vydání 2005
  - Agenda spotřeby
  - Statistický modul, vypočty trendů
  - Integrace s ostatními mikrobiologickými aplikacemi
  - Integrace s místním kontextem lékárny a žádanek
  - Agenda antiobiotických přípravků
  - Centrální správa konfiguračních údajů

E.Agenda evidence kmenů

- Provozní infrastruktura – identická se sub A.
- Speciální software ve verzi 2003, vydání 2005
  - Agenda evidence kmenů s vazbou na SZÚ
  - Integrace do centralizovaných studií
  - Centrální správa konfiguračních údajů
  - Integrace s ostatními mikrobiologickými aplikacemi

F.Žádankový systém pro vázaná antibiotika

- Provozní infrastruktura – identická se sub A.
- Speciální software ve verzi 1999, vydání 2005
  - Agenda žádanek
  - Integrace do konzultačního systému
  - Integrace s ostatními mikrobiologickými aplikacemi

G.Auditovací systém

- Provozní infrastruktura – identická se sub A.
- Speciální software ve verzi 2005
  - Interaktivní taxování vůči autoritativně definované správné praxi při léčbě antibiotiky.

Příloha 1 – Taxativní výčet poskytovaných a servisovaných komponent a služeb

A.Laboratorní systém pro mikrobiologii, serologii a virologii

- Provozní infrastruktura
  - Technické vybavení – 2ks provozní server, provozní a záložní. Kapacita dostatečná pro 5 let provozu á 100,000 přijatých vzorků ročně.
  - VaxNt - licence pro provoz v rámci dodávaného systému, webová část systému využitelná v rámci celé nemocnice bez omezení. VaxNt zahrnuje software, dokumentaci i interpretační modul pro zákaznicky definovaný provoz. Konfigurace pro ekonomické využití, evidenci klientely a další specifické agendy je součástí dodávky v referenční podobě.
  - Web server prezentační i transportní
  - File / print server
  - Automatický zálohovací systém
  - Systém zotavení z havárie
- Speciální software ve verzi 2001, vydání 2005.
  - Provozní systém - včetně referenční konfigurace, číselníků apod.
    - Evidenční systém / příjmový protokol
    - Mikrobiologická kniha
    - Vývojové prostředky
    - Generátor výsledků
    - Generátor web stránek
    - Inteligentní spooler pro tisk
    - Pomocné programy pro tisky štítků apod.
    - Účtovací subsystém včetně úprav pro místní kontext
    - Generátor kumulativních výsledků
    - Periodický import provozních údajů do statistických databází
    - Obecné ekonomické moduly na bázi VaxNt
    - Zprovoznění na místě
    - Zprovoznění aplikačního serveru
    - Zprovoznění rozhraní na nemocniční systém (technické propojení)
    - Konfigurace až 10 ks laboratorních PC
    - Úprava identifikačních a konfiguračních údajů
    - Servis a technická podpora serveru a aplikací
    - Získávání nových verzí systému.
    - Zakomponování systému do širšího okolí
    - Úpravy účetního rozhraní podle specifikací
    - Úpravy prezentačního rozhraní pro odebírání výsledků ostatními subsystémy v nemocnici.
    - Export účetních údajů v jednoduchém formátu jako textový soubor a rozhraní na registr rovněž přes aktualizovaný textový soubor.
    - Prezentace přes web je rovnou součástí systému.

B.Agenda nemocničních a komunitních infekcí

- Provozní infrastruktura – identická se sub A.
- Speciální software ve verzi 2003, vydání 2005.
  - Rutinní agenda
  - Evidence suspektních případů
  - Kauzy kontroly infekcí
  - Agenda kontroly infekcí
  - Statistický modul
  - Všeobecně přístupné rozhraní pro potřeby intervencí
  - Integrace s agendou laboratorního systému

Předávací protokol
laboratorního informačního systému mikrobiologie

Ve smyslu smlouvy č. 177/2005 ze 4. dubna 2005 předáváme laboratorní informační systém pro mikrobiologickou laboratoř Všeobecné fakultní nemocnice v Praze.

Dodány a zprovozněny byly:

A. Laboratorní systém pro mikrobiologii, serologii a virologii

- Provozní infrastruktura
  - Technické vybavení – 2ks provozní server, provozní a záložní. Kapacita dostatečná pro 5 let provozu á 100,000 přijatých vzorků ročně.
  - VaxNt - licence pro provoz v rámci dodávaného systému, webová část systému využitelná v rámci celé nemocnice bez omezení. VaxNt zahrnuje software, dokumentaci i interpretační modul pro zákaznicky definovaný provoz. Konfigurace pro ekonomické využití, evidenci klientely a další specifické agendy je součástí dodávky v referenční podobě.
  - Web server prezentační i transportní
  - File / print server
  - Automatický zálohovací systém
  - Systém zotavení z havárie
- Speciální software ve verzi 2001, vydání 2005.
  - Provozní systém - včetně referenční konfigurace, číselníků apod.
    - Evidenční systém / příjmový protokol
    - Mikrobiologická kniha
    - Vývojové prostředky
    - Generátor výsledků
    - Generátor web stránek
    - Inteligentní spooler pro tisk
    - Pomocné programy pro tisky štítků apod.
    - Účtovací subsystém včetně úprav pro místní kontext
    - Generátor kumulativních výsledků
    - Periodický import provozních údajů do statistických databází
    - Obecné ekonomické moduly na bázi VaxNt
    - Zprovoznění na místě
    - Zprovoznění aplikačního serveru
    - Zprovoznění rozhraní na nemocniční systém (technické propojení)
    - Konfigurace až 10 ks laboratorních PC
    - Úprava identifikačních a konfiguračních údajů
    - Servis a technická podpora serveru a aplikací
    - Získávání nových verzí systému.
    - Zakomponování systému do širšího okolí
    - Úpravy účetního rozhraní podle specifikací
    - Úpravy prezentačního rozhraní pro odebírání výsledků ostatními subsystémy v nemocnici.
    - Export účetních údajů v jednoduchém formátu jako textový soubor a rozhraní na registr rovněž přes aktualizovaný textový soubor.
    - Prezentace přes web je rovnou součástí systému.

B. Agenda nemocničních a komunitních infekcí

- Provozní infrastruktura – identická se sub A.
- Speciální software ve verzi 2003, vydání 2005.
  - Rutinní agenda
  - Evidence suspektních případů

- Kauzy kontroly infekcí
- Agenda kontroly infekcí
- Statistický modul
- Všeobecně přístupné rozhraní pro potřeby intervencí
- Integrace s agendou laboratorního systému

C.Konzultační systém pro antibiotickou terapii

- Provozní infrastruktura – identická se sub A.
- Speciální software ve verzi 2005
  - Agenda konzultací
  - Optimalizace léčby
  - Statistický modul
  - Integrace s ostatními mikrobiologickými aplikacemi
  - Agenda antiobiotických přípravků

D.Agenda spotřeby antibiotik

- Provozní infrastruktura – identická se sub A.
- Speciální software ve verzi 2003, vydání 2005
  - Agenda spotřeby
  - Statistický modul, vypočty trendů
  - Integrace s ostatními mikrobiologickými aplikacemi
  - Integrace s místním kontextem lékárny a žádanek
  - Agenda antiobiotických přípravků
  - Centrální správa konfiguračních údajů

E.Agenda evidence kmenů

- Provozní infrastruktura – identická se sub A.
- Speciální software ve verzi 2003, vydání 2005
  - Agenda evidence kmenů s vazbou na SZÚ
  - Integrace do centralizovaných studií
  - Centrální správa konfiguračních údajů
  - Integrace s ostatními mikrobiologickými aplikacemi

F.Žádankový systém pro vázaná antibiotika

- Provozní infrastruktura – identická se sub A.
- Speciální software ve verzi 1999, vydání 2005
  - Agenda žádanek
  - Integrace do konzultačního systému
  - Integrace s ostatními mikrobiologickými aplikacemi

G.Auditovací systém

- Provozní infrastruktura – identická se sub A.
- Speciální software ve verzi 2005
  - Interaktivní taxování vůči autoritativně definované správné praxi při léčbě antibiotiky.

Pracovníky zhotovitele bylo provedeno zprovoznění rozhraní na nemocniční systém (technické propojení) VFN v Praze.

Dále byla nastavena konfigurace vybraných laboratorních PC, zprovozněny statistické funkce a provedena úprava identifikačních konfiguračních údajů.

Zástupci zhotovitele (ing. Dalibor Straka) a uživatele (prim.MUDr.A.Jedličková) prohlašují, že neshledali žádné překážky bránící předání a převzetí laboratorního informačního systému mikrobiologie a na základě této shody podepisují předávací protokol.

V Praze dne dne 3. července 2006

Za zhotovitele : [redacted]

Za uživatele : [redacted]

Dodatek č. 1
Smlouvy č. PO 263/S/05

Janiga Labs, s.r.o.
se sídlem: Jinočanská 251/4, PSČ: 161 00, Praha 6
IČO: 639 90 148
DIČ: CZ63990148
bankovní spojení: [redacted]
číslo účtu:
zapsaná v obchodním rejstříku Městského soudu v Praze v oddílu C vložka 38795,
zastoupená Marcelem Valešem, jednatelem společnosti

jako Poskytovatel na straně jedné (dále jen „Poskytovatel")

a

Všeobecná fakultní nemocnice v Praze
se sídlem: U Nemocnice 499/2, PSČ: 128 08, Praha 2
IČO: 000 64 165
DIČ: CZ00064165
bankovní spojení: Česká národní banka
číslo účtu: 24035021/0710
zastoupená prof. MUDr. Davidem Feltlem, Ph.D., MBA, ředitelem nemocnice

jako Objednatel na straně druhé (dále jen „Objednatel")

uzavřeli dnešního dne, měsíce a roku ke smlouvě o poskytnutí a servisu informačního systému mikrobiologie ze dne 4. 4. 2002, která je u Objednatele evidována pod sp. zn. PO 263/S/05 (dále jen „smlouva") tento

D O D A T E K Č. 1
(dále též „dodatek")

I.
Předmět dodatku

1. Na základě dohody smluvních stran se znění smlouvy č. PO 263/S/05 (u Poskytovatele evidována pod č. 177/2005) mění a zcela nahrazuje zněním následujícím:

Smlouva o poskytnutí a servisu informačního systému, mikrobiologie
(dále též „smlouva")

Smluvní strany

Janiga Labs, s.r.o.
se sídlem: Jinočanská 251/4, 161 00 Praha 6
IČO: 639 90 148
DIČ: CZ63990148
bankovní spojení: [redacted]
číslo účtu:
zapsaná v obchodním rejstříku Městského soudu v Praze v oddílu C vložka 38795,
zastoupená jednatelem společnosti Marcelem Valešem,
jako Poskytovatel na straně jedné (dále jen „Poskytovatel")

a

Všeobecná fakultní nemocnice v Praze
se sídlem: U Nemocnice 499/2, PSČ: 128 08, Praha 2
IČO: 000 64 165
DIČ: CZ00064165
bankovní spojení: Česká národní banka
číslo účtu: 24035021/0710
zastoupená ředitelem nemocnice prof. MUDr. Davidem Feltlem, Ph.D., MBA,
jako Objednatel na straně druhé (dále jen „Objednatel")

Článek I.
Vymezení základního pojmosloví

1. Objednatelem a uživatelem je podle této smlouvy Všeobecná fakultní nemocnice v Praze tak, jak je uvedeno v záhlaví této smlouvy.

2. Poskytovatelem je podle této smlouvy Janiga Labs, s.r.o., tak, jak je uvedeno v záhlaví této smlouvy.

Článek II.
Předmět plnění

1. Předmětem plnění je dle této smlouvy poskytnutí licencí a zabezpečení servisu k informačnímu systému, jehož komponenty jsou jmenovitě:

   A. Laboratorní systém pro mikrobiologii, sérologii a virologii
   B. Agenda nemocničních a komunitních infekci
   C. Konzultační systém pro antibiotickou terapii
   D. Agenda spotřeby antibiotik
   E. Agenda evidence kmenů
   F. Žádankový systém pro vázaná antibiotika
   G. Auditovací systém

2. Smluvní strany berou na vědomí, že výčet blíže specifikovaný v čl. II odst. 1 této smlouvy je pouze výčtem demonstrativním, pročež taxativní výčet poskytnutých komponent je uveden v Příloze č. 1 této smlouvy, která je její nedílnou součástí. Komponenty budou Poskytovatelem Objednateli poskytnuty včetně specifické konfigurace, implementace do místního prostředí informačních systémů a zaškolení příslušného personálu.

3. Rozhraním na celonemocniční informační systém se dále rozumí výměna vyúčtovacích dat, žádanek, výsledků a statistik. Technická implementace rozhraní bude realizována Poskytovatelem podle konkrétní specifikace Objednatele, výměna dat v obou směrech bude implementována JDBC konektivitou nebo některým z protokolů nfs, smb, ssh či ftp a to formou textových nebo XML dokumentů.

4. Časové a reakční lhůty servisu: Reakční doby a doby odstranění závad ze strany Poskytovatele jsou stanoveny v Příloze č. 2 této smlouvy. Hlášení závad, chyb, provozních problémů a požadavků je prováděno prostřednictvím elektronického zadání 24x7 v helpdesku Objednatele nebo telefonicky na uvedených telefonických kontaktních číslech:

   - v pracovních dnech mezi 9:00 a 16:00 kontakty Helpdesk viz příloha č.4
   - mimo pracovní dny na číslech a v naléhavých případech kontakty Helpdesk viz příloha č.4

   Dojde-li ke změně telefonních čísel Poskytovatele, bude o tom Objednatel neprodleně informován.

5. Servis se nevztahuje na závady způsobené zejména neodbornou či nevhodnou manipulaci s technickým vybavením, úmyslným poškozením, krádeží, Objednatelem neautorizovanými zásahy, zásahem vyšší moci nebo provozováním systému v nevyhovujících podmínkách. Servis se také nevztahuje na technické závady a na závady operačního systému pracovních stanic či síťové infrastruktury Objednatele. Poskytovatel se nicméně zavazuje k poskytnutí nezbytných informací o vhodné konfiguraci počítačů v případě, že Objednatel bude nucen počítače po odstranění technické závady rekonfigurovat a znovu zprovoznit. Servis virtuálních serverů nezahrnuje provozní, bezpečnostní správu a řešení incidentů. Servis/maitenance se nevztahuje na další aplikace zakoupené mimo tuto smlouvu.

6. Servis se výslovně vztahuje na tyto činnosti:

   a. Poskytování nových verzí systému i provozní infrastruktury včetně instalace.
   b. Pomoc při akceptování konfiguračních souborů, programovatelných formulářů a dalších komponent systému vznikajících průběžně v referenční verzi systému.
   c. Dohled a údržba operačního systému provozního serveru.
   d. Průběžná správa serverové aplikace JLABS MBIO, jeho součástí a proaktivní detekce provozních problémů.
   e. Konzultace nebo vyžádané úpravy konfiguračních dat a programových skriptů v rozsahu do dvou hodin měsíčně.

7. Poskytovatel se stává plněním dle této Smlouvy Poskytovatelem systémů, technologií a služeb, na kterých je provozována základní služba: Poskytování zdravotních služeb dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „ZKB"). Objednatel je orgánem nebo osobou provozující základní službu podle ZKB § 3 písm. f) a provozování základní služby Objednatelem podle ZKB je závislé na provozování řešení poskytovaného Poskytovatelem.

8. Objednatel jmenuje odpovědným pracovníkem ve věci koordinace vyžádaného servisu systému primářku MUDr. Václavu Adámkovou, Ph.D. s oprávněním schválit a převzít servisní zásahy.

Článek III.
Dohoda o ceně a způsob platby

1. Cena za servis systému je stanovena dohodou smluvních stran ve výši 604.440,- Kč bez DPH ročně. Cena bude zatížena DPH v aktuálně platné sazbě. Cena servisu bude upravena každý rok v dubnu oficiálním indexem spotřebitelských cen vyhlášeným ČNB k 31. březnu, a to formou dodatku k této smlouvě. Datum podepsání dodatku nemá odkladný účinek aktualizované fakturace.

2. Fakturace proběhne vždy k 1. červenci daného roku s tím, že splatnost faktur je 60 dní.

3. Smluvní strany berou na vědomí, že faktury musí splňovat veškeré, zákonem stanovené předpoklady, pročež v případě chybného vystavení faktury má Objednatel právo ve lhůtě 15 dnů ode dne doručení faktury tuto vrátit Poskytovateli

k opravě. Po provedení opravy předmětné faktury zašle tuto Poskytovatel k rukám Objednatele, přičemž tímto počíná běh nové lhůty splatnosti ve smyslu čl. III odst. 2 této smlouvy.

Článek IV.
Místo plnění

1. Místo plnění je shodné se sídlem Objednatele, uvedeným v záhlaví této smlouvy.

2. Objednatel se zavazuje zabezpečit Poskytovateli vzdálený i fyzický přístup k poskytovanému systému pro potřeby servisu a případné implementace nových technologií či postupů.

3. V případě vzdáleného přístupu se při plnění této smlouvy Poskytovatel zavazuje dodržovat povinnosti uvedené v dokumentu „SM-UI-02 Používání sítě VFN externími uživateli", který je Přílohou č. 3 této smlouvy.

Článek V.
Platnost smlouvy

1. Tato smlouva nabývá platnosti dnem jejího podpisu oběma stranami a účinnosti v souladu se zákonem č. 340/2015, o registru smluv, ve znění pozdějších předpisů. Smlouva se uzavírá na dobu určitou, tedy na dobu tří let ode dne účinnosti této smlouvy, pročež výpovědní lhůta činí 12 měsíců pro obě strany.

2. Nebude-li smlouva písemně vypovězena ani jednou ze smluvních stran alespoň 12 měsíců před předpokládaným datem ukončení smlouvy, prodlužuje se platnost automaticky vždy o dalších 12 měsíců.

3. Platnost této smlouvy může být také ukončena po vzájemné písemné dohodě smluvních stran.

4. Smluvní strany mají rovněž právo od smlouvy odstoupit v případě hrubého porušení smlouvy, za kterézto smluvní strany označují:

    a. Neuhrazení ceny ve smyslu čl. III této smlouvy ze strany Objednatele;

    b. Opakované pozdní či chybné dodání předmětu plnění Objednateli ve smyslu čl. II této smlouvy.

Článek VI.
Závazky Objednatele

1. Objednatel se zavazuje zaplatit Poskytovateli dohodnutou cenu za služby poskytnuté dle této smlouvy.

2. Objednatel se zavazuje zajistit Poskytovateli jím požadované potřebné informace věcného i systémového charakteru pro plnění této smlouvy.

3. Objednatel zajistí ve svém prostředí pro Poskytovatele technologickou infrastrukturu v rozsahu virtuální server, vzdálený přístup, síťová infrastruktura a koncové stanice a zajistit jejich provoz.

4. Objednatel je povinen určit oprávněné osoby pro styk s Poskytovatelem, které budou po dobu platnosti této smlouvy zabezpečovat nezbytnou součinnost mezi Poskytovatelem a Objednatelem a k zajištění potřebných informací a materiálů k plnění této smlouvy. Objednatel může tyto oprávněné osoby zaměnit jinými, které budou vhodné pro výkon prací, a to po předchozím písemném vyrozumění Poskytovatele (seznam oprávněných osob je Přílohou č. 4 této smlouvy).

5. Oprávněné osoby Objednatele odpovídají za obsah a správnost předaných požadavků a informací.

Článek VII.
Závazky Poskytovatele

1. Poskytovatel se zavazuje plnit své povinnosti vyplývající z této smlouvy s maximální odpovědností, a to tak, aby systém byl udržován nepřetržitě v provozuschopném, funkčním stavu za předpokladu dodržení závazků Objednatele. Poskytovatel odpovídá za kvalitu a včasnost vykonaných prací ve smyslu výše uvedených ustanovení.

2. Poskytovatel je povinen systém zabezpečit tak, aby k jím obsahovaným údajům měly přístup pouze a jenom osoby určené Objednatelem Za jakékoli škody, s výjimkou fyzického poškození serverů, způsobené Objednateli zásahem neoprávněně přihlášené osoby odpovídá Poskytovatel.

3. Poskytovatel je odpovědný za majetkovou a nemajetkovou újmu, která Objednateli vznikne prokazatelným neplněním nebo vadným plněním jeho závazků vyplývajících z této smlouvy.

4. Poskytovatel neodpovídá za jakékoli škody, opožděná nebo neposkytnutá plnění, pokud toto bude zapříčiněno neplněním závazků Objednatele uvedených v bodech 2. – 5. článku VI. Této smlouvy nebo zásahem třetí strany do systému. Rozsah potřebných informací požadovaných Poskytovatelem specifikuje Objednateli Poskytovatel, a to po nahlášení nebo potvrzení přijetí požadavku.

5. Poskytovatel musí Objednatele skrze odpovědnou osobu neprodleně informovat o kybernetických bezpečnostních incidentech souvisejících s poskytovaným řešením, pročež smluvní strany za tuto osobu označují: manažera kybernetické bezpečnosti, e-mail: [redacted]

6. Poskytovatel je povinen Objednatele informovat prostřednictvím manažera kybernetické bezpečnosti o způsobu řízení rizik na straně Poskytovatele a o zbytkových rizicích souvisejících s plněním Smlouvy v půl ročním intervalu nebo v případě zjištění nových rizik nebo změn stávajících rizik informovat bezodkladně.

7. Poskytovatel je povinen informovat manažera kybernetické bezpečnosti Objednatele o významné změně v ovládání Poskytovatele nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných Poskytovatel k plnění podle této Smlouvy.

8. Poskytovatel bere na vědomí, že služby poskytované dle této Smlouvy nesmí být provozované na technických nebo programových prostředcích označených NÚKIB jako hrozba.

9. Poskytovatel je povinen určit oprávněné osoby pro styk s Objednatelem, které budou po dobu platnosti této smlouvy zabezpečovat nezbytnou součinnost mezi Objednatelem a Poskytovatelem a k zajištění potřebných informací a materiálů k plnění této smlouvy. Poskytovatel může tyto oprávněné osoby zaměnit jinými, které budou vhodné pro výkon prací, a to po předchozím odsouhlasení Objednatelem (seznam oprávněných osob je Přílohou č. 4 této smlouvy).

10. Poskytovatel se zavazuje splňovat/dodržet relevantní požadavky na řízení bezpečnosti informací uvedené v Příloze č. 5 této smlouvy „Požadavky systému řízení bezpečnosti informací na dodavatele" vztahující se na prostředí a činnosti Poskytovatele.

VIII.
Smluvní pokuty, sankce

1. Pro případ prodlení Objednatele s úhradou ceny dle čl. IV této smlouvy má Poskytovatel nárok na zaplacení úroku z prodlení ze strany Objednatele ve výši 0,01 % z částky, s jejíž platbou je Objednatel v prodlení, za každý den takového prodlení. Smluvní strany se dohodly, že Poskytovatel je oprávněn požadovat zaplacení úroku z prodlení až po uplynutí 30 dnů od sjednané lhůty splatnosti.

2. V případě nedodržení podpory na úrovni minimálně SLA 99,93 % je Objednatel oprávněn požadovat jednorázovou smluvní pokutu ve výši 5.000,- Kč za každý jednotlivý případ.

3. V případě překročení maximální doby 2 hodin neplánované odstávky SW řešení je Objednatel oprávněn požadovat smluvní pokutu ve výši 5.000,- Kč a 1.000,- Kč za každou i započatou hodinu nad limit 2 hodin za každý jednotlivý případ.

4. V případě havárie, pokud jsou plněny závazky Objednatele, je Objednatel oprávněn za nedodržení termínu pro odstranění závady uvedeného v Tabulce č. 1 v bodě 1 Přílohy č. 2 této smlouvy požadovat jednorázovou smluvní pokutu ve výši 5.000,- Kč a 1.000,- Kč za každou i započatou hodinu prodlení za každý jednotlivý případ.

5. V případě chyby je Objednatel oprávněn za nedodržení termínu uvedeného v Tabulce č. 1 v bodě 2 Přílohy č. 2 této smlouvy požadovat jednorázovou smluvní pokutu ve výši 2.000,- Kč a 1.000,- Kč za každý i započatý pracovní den prodlení za každý jednotlivý případ.

6. V případě nedodržení povinností Poskytovatele dle čl. IX této smlouvy, má Objednatel právo účtovat Poskytovateli smluvní pokutu ve výši 100 000,- Kč za každé jednotlivé porušení povinnosti.

7. V případě sankcí nebo jiných finančních dopadů z poskytované podpory vyplývající z porušení nebo nedodržení povinností a náležitostí ZKB způsobené Poskytovatelem má Objednatel právo účtovat Poskytovateli smluvní pokutu ve výši 100.000,- Kč za každé jednotlivé porušení povinnosti.

8. Na výše uvedené smluvní pokuty nemá Objednatel nárok, prokáže-li se, že havárie nebo chyba byla způsobena jednáním Objednatele, selháním techniky na straně Objednatele nebo jiným neplněním závazků Objednatele.

9. Uplatněním nároku na zaplacení smluvní pokuty ani jejím skutečným uhrazením nezanikne povinnost Poskytovatele splnit povinnost, jejíž plnění bylo zajištěno smluvní pokutou, a Poskytovatel tak bude nadále povinen ke splnění takovéto povinnosti.

10. Smluvní pokuta bude vyúčtovaná samostatným daňovým dokladem, splatnost smluvní pokuty činí 30 dní ode dne doručení vyúčtování Poskytovateli.

11. Zaplacením smluvní pokuty není dotčen nárok Objednatele na náhradu škody, včetně náhrady škody, která převyšuje smluvní pokutu.

Článek IX.
Mlčenlivost

1. Poskytovatel se zavazuje zachovávat mlčenlivost ve vztahu ke všem informacím a skutečnostem, které se dozví o Objednateli, jeho zaměstnancích, pacientech atd. v souvislosti s uzavřením a plněním smlouvy, pokud tyto informace mají povahu obchodního tajemství, osobních údajů nebo mají být z jiných důvodů chráněny před zveřejněním. Poskytovatel je povinen nakládat s osobními údaji a zejména s údaji o zdravotním stavu, genetickými a biometrickými údaji (dále jen

„Osobní údaje") v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 (dále jen GDPR) a příslušnými ustanoveními zákona č. 110/2019 Sb., o zpracování osobních údajů.

2. Povinnost mlčenlivosti platí rovněž o skutečnostech, na něž se vztahuje povinnost mlčenlivosti pracovníků Objednatele, zejména podle ustanovení § 51 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (Zákon o zdravotních službách), a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení Osobních údajů.

3. Pokud Poskytovatel přijde při plnění Smlouvy do styku s Osobními údaji a bude v postavení zpracovatele ve smyslu GDPR 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 GDPR se Zákonem o zpracování osobních údajů a Zákonem o zdravotních službách. Zpracovávání Osobních údajů v rozsahu údajů poskytnutých Objednatelem a týkajících se zdravotnické dokumentace pacientů, jimž jsou Objednatelem poskytovány zdravotní služby, a dále v rozsahu osobních údajů zaměstnanců Objednatele, kteří jsou Poskytovateli zdravotních služeb Poskytovatele, může zahrnovat odstranění potíží za účelem zabránění, vyhledávání a opravy problémů zjištěných při poskytování Služby, může také zahrnovat zlepšování funkcí informačních systémů, vyhledávání hrozeb uživatelům a ochrany uživatelů informačních systémů. Osobní údaje nebudou použity k jinému účelu, ani z nich nebudou odvozovány informace pro žádné reklamní či jiné komerční účely. Poskytovatel za účelem ochrany Osobních údajů Objednatele a jeho pacientů, zaměstnanců a 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 GDPR a Zákona o zpracování osobních údajů, zejména zajistí, aby data obsažená ve zdravotnické dokumentaci byla zabezpečena způsobem, který znemožní nahlížení do této zdravotnické dokumentace neoprávněným osobám.

4. Smluvní strany jsou povinny zajistit, že nebudou neoprávněně pořizovány kopie informací či jiné záznamy dle této smlouvy, a nebudou zjišťovány informace, které nejsou nezbytně nutné ke splnění povinností vyplývajících z této smlouvy.

5. Smluvní strany se zavazují pro případ, že se v průběhu plnění dle této smlouvy dostanou do kontaktu s údaji druhé smluvní strany vyplývajícími z její provozní činnosti, tyto údaje v žádném případě nezneužít, nezměnit ani jinak nepoškodit, neztratit či neznehodnotit.

6. Poskytovatel se zejména zavazuje, že nepoužije jakýkoliv Osobní údaj, s nímž přijde do styku při plnění závazků dle Smlouvy, a ani neumožní jeho použití třetí osobě.

7. Poskytovatel se zavazuje plně respektovat bezpečnostní požadavky Objednatele k zajištění ochrany Osobních údajů pacientů a klientů Objednatele.

8. Poskytovatel se zavazuje zajistit informovanost svých pracovníků o povinnostech vyplývajících z této Smlouvy. Poskytovatel se zavazuje zajistit, aby jeho zaměstnanci a/nebo Poddodavatelé přicházející při výkonu své práce do styku s Osobními údaji pacientů, zaměstnanců a klientů Objednatele, byli náležitě poučeni o povoleném způsobu nakládání s takovými údaji a byli seznámeni s následky jednání, které by bylo v rozporu se zákonnou úpravou a bezpečnostními směrnicemi Objednatele, s nimiž byli prokazatelně seznámeni. Poskytovatel se zavazuje informovat své poddodavatele o povinnosti mlčenlivosti dle této smlouvy. V případě porušení mlčenlivosti za strany poddodavatele, odpovídá Poskytovatel Objednateli za vzniklou škodu, jako kdyby povinnost porušil sám.

9. Povinnost mlčenlivosti o informacích a skutečnostech obchodního charakteru trvá po dobu 5 let od ukončení účinnosti této smlouvy, o informacích obsahujících Osobní údaje trvá bez časového omezení.

Článek X.
Součinnost v případě ukončení provozu SW řešení

1. Poskytovatel za účelem řádného a plynulého převedení v případě ukončení smlouvy všech činností spojených se servisem a podporou řešení především:

   - poskytne za úplatu, podle rozsahu požadovaných prací, náležitou a nezbytnou součinnost pro takové převedení,
   - poskytne veškeré nezbytné informace a dokumentaci,
   - data ve stávajícím formátu budou Objednateli předána bezúplatně, pokud bude Objednatel požadovat jiný formát dat, mohou být práce související s převodem dat do požadovaného formátu zpoplatněny,
   - na žádost Objednatele provede protokolární likvidaci dat a provozních údajů souvisejících s poskytováním údržby SW řešení a tímto zanikne možnost vedení jakéhokoliv i budoucího sporu.

Článek XI.
Ostatní ujednání

1. Poskytovatel bere na vědomí, že Objednatel je povinen dle ustanovení § 219 z. č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění a dle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů, zveřejnit tuto smlouvu včetně případných dodatků zákonem stanoveným způsobem. Mlčenlivost se tak nevztahuje na tyto informace.

2. Poskytovatel se zavazuje dodržovat nařízení Objednatele, kterým je zakázáno kouření ve všech prostorách i plochách areálu Objednatele s výjimkou vyhrazených prostor.

3. Poskytovatel je oprávněn postoupit pohledávku vyplývající z plnění dle této smlouvy na třetí osobu pouze s předchozím písemným souhlasem Objednatele.

4. Obě strany se zavazují, že v souvislosti s plněním smlouvy učiní opatření k zajištění ochrany před šířením počítačových virů a nelegálních programů.

5. Poskytovatel prohlašuje, že zajištěním podpory systému pro Objednatele neporušuje práva třetích osob ve smyslu autorského zákona či jiných právních předpisů a že tak činí v souladu s autorským zákonem.

6. Poskytovatel je povinen mít v platnosti a udržovat pojištění odpovědnosti za škodu způsobenou zadavateli či třetím osobám při výkonu podnikatelské činnosti, která je předmětem této smlouvy, s limitem pojistného plnění v minimální výši 1.000.000,- Kč.

7. Poskytovatel je povinen udržovat výše uvedené pojištění po celou dobu trvání smlouvy. V případě porušení této povinnosti je zadavatel oprávněn od smlouvy, která bude uzavřena na základě výsledku tohoto zadávacího řízení odstoupit. Na žádost zadavatele je Poskytovatel povinen předložit zadavateli dokumenty prokazující, že pojištění v požadovaném rozsahu a výši trvá. Pokud by v důsledku pojistného plnění nebo jiné události mělo dojít k zániku pojistného, k omezení rozsahu pojištěných rizik, ke snížení stanovené min. výše pojistného v pojištění, nebo k jiným změnám, které by znamenaly zhoršení podmínek oproti původnímu stavu, je Poskytovatel povinen učinit příslušná opatření tak, aby pojištění bylo udrženo tak, jak je požadováno v tomto ustanovení.

Článek XII.
Závěrečná ustanovení

1. Změny a doplňky této smlouvy jsou přípustné pouze v písemné formě na základě dohody obou stran.

2. Smluvní strany se dohodly, že jejich závazkový vztah založený touto smlouvou se bude řídit zákonem č. 89/2012 Sb., občanským zákoníkem, v platném znění (dále též „OZ").

3. Pokud není v této smlouvě sjednáno jinak, řídí se práva a povinnosti smluvních stran příslušnými ustanoveními OZ.

4. Smlouva je vyhotovena ve 4 stejnopisech, z nichž každá strana obdrží po 2 exemplářích.

5. Obě smluvní strany prohlašují, že tuto smlouvu uzavřely na základě vzájemné dohody podle své pravé a svobodné vůle. Toto stvrzují svým vlastnoručním podpisem

6. Na základě dohody smluvních stran se rovněž mění veškeré původní přílohy smlouvy č. PO 263/S/05 (u Poskytovatele evidována pod č. 177/2005), pročež tyto nově znějí:

Přílohy:
Příloha č. 1 - Taxativní výčet poskytovaných a servisovaných komponent a služeb
Příloha č. 2 - Specifikace podpory SW řešení
Příloha č. 3 - SM-UI-02 Používání sítě VFN externími uživateli
Příloha č. 4 - Seznam oprávněných osob
Příloha č. 5 - Požadavky systému řízení bezpečnosti informací na dodavatele
Příloha č. 6 - Průběh inflace

V Praze dne ……

V Praze dne……..

Všeobecná fakultní nemocnice v Praze
prof. MUDr. David Feltl, Ph.D., MBA, ředitel

Janiga Labs, s.r.o.
Marcel Valeš, jednatel

Příloha č. 1

Taxativní výčet poskytovaných a servisovaných komponent a služeb

Laboratorní systém pro mikrobiologii, sérologii a virologii

- Provozní infrastruktura
  - VaxNt – licence pro provoz v rámci dodávaného systému, webová část systému využitelná v rámci celé nemocnice bez omezení. VaxNt zahrnuje software, dokumentaci i interpretační modul pro zákaznicky definovaný provoz. Konfigurace pro ekonomické využití, evidenci klientely a další specifické agendy je součástí dodávky v referenční podobě.
  - Automatický zálohovací systém
  - Systém zotavení z havárie
- Speciální software ve verzi 2001, vydání 2005.
  - Provozní systém – včetně referenční konfigurace, číselníků apod.
    - Evidenční systém / příjmový protokol
    - Mikrobiologická kniha
    - Vývojové prostředky
    - Generátor výsledků
    - Generátor web stránek
    - Inteligentní spooler pro tisk
    - Pomocné programy pro tisky štítků apod.
    - Účtovací subsystém včetně úprav pro místní kontext
    - Generátor kumulativních výsledků
    - Periodicky import provozních údajů do statistických databází
    - Obecné ekonomické moduly na bázi VaxNt
    - Zprovoznění na místě
    - Zprovoznění aplikačního serveru
    - Zprovoznění rozhraní na nemocniční systém (technické propojení)
    - Konfigurace až 10 ks laboratorních PC
    - Úprava identifikačních a konfiguračních údajů
    - Servis a technická podpora serveru a aplikací
    - Získávání nových verzí systému.
    - Zakomponování systému do širšího okolí
    - Úpravy účetního rozhraní podle specifikací
    - Úpravy prezentačního rozhraní pro odebírání výsledků ostatními subsystémy v nemocnici.
    - Export účetních údajů v jednoduchém formátu jako textový soubor a rozhraní na registr rovněž přes aktualizovaný textový soubor.
    - Prezentace přes web je rovnou součástí systému.

Agenda nemocničních a komunitních infekcí

- Provozní infrastruktura — identická se sub A.
- Speciální software ve verzi 2003, vydání 2005.
  - Rutinní agenda
  - Evidence suspektních případů
  - Kauzy kontroly infekcí
  - Agenda kontroly infekcí
  - Statistický modul
  - Všeobecně přístupné rozhraní pro potřeby intervencí
  - Integrace s agendou laboratorního systému

Konzultační systém pro antibiotickou terapii

- Provozní infrastruktura — identická se sub A.
- Speciální software ve verzi 2005
  - Agenda konzultací
  - Optimalizace léčby
  - Statistický modul
  - Integrace s ostatními mikrobiologickými aplikacemi
  - Agenda antibiotických přípravků

Agenda spotřeby antibiotik

- Provozní infrastruktura — identická se sub A.
- Speciální software ve verzi 2003, vydání 2005
  - Agenda spotřeby
  - Statistický modul, výpočty trendů
  - Integrace s ostatními mikrobiologickými aplikacemi
  - Integrace s místním kontextem lékárny a žádanek

    - Agenda antibiotických přípravků
    - Centrální správa konfiguračních údajů

Agenda evidence kmenů

- Provozní infrastruktura — identická se sub A.
- Speciální software ve verzi 2003, vydání 2005
    - Agenda evidence kmenů s vazbou na SZÚ
    - Integrace do centralizovaných studií
    - Centrální správa konfiguračních údajů
    - Integrace s ostatními mikrobiologickými aplikacemi

Žádankový systém pro vázaná antibiotika

- Provozní infrastruktura — identická se sub A.
- Speciální software ve verzi 1999, vydání 2005
    - Agenda žádanek
    - Integrace do konzultačního systému
    - Integrace s ostatními mikrobiologickými aplikacemi

Auditovací systém

- Provozní infrastruktura — identická se sub A.
- Speciální software ve verzi 2005
    - Interakční taxování vůči autoritativně definované správné praxi při léčbě antibiotiky.

Příloha č. 2

Specifikace podpory dodaného SW řešení

1. Podpora dostupnosti systému 24x7

   Podpora běhu SW aplikace, databáze a OS, instalace nových verzí, aktualizací v souladu s platnou legislativou, nasazení patchů a hotfixů.
   Zajištění dostupnosti 24x7 – SLA 99,93%
   Odstávky systému je nezbytné plánovat s odpovědnými pracovníky Objednatele.
   Max. doba neplánované odstávky: **2 hodiny**

   Není omezeno počtem odpracovaných hodin.

2. Uživatelská podpora
   Hlášení závad, chyb, provozních problémů a požadavků:
   - Hotline (telefonické zadání) – **24x7,** viz kontaktní čísla uvedená v Příloze č.4.
   - Helpdesk (elektronické zadání) – **24x7,** evidence je realizována v helpdesku Objednatele.

   Tabulka č. 1

Bod	Úroveň / závažnost závady	Maximální reakční doba	Maximální doba odstranění závady
1	Havárie	4 hodiny	24 hodin
2	Chyba	8 hodin	7dní

   Havárie: je stav, kdy dodané SW řešení dle předmětu smlouvy není funkční, tzn. SW neumožňuje náhradní ani dočasné řešení.

   Chyba: Stav, kdy SW řešení neplní některou dílčí funkci uvedenou v provozní nebo uživatelské dokumentaci, a lze ji nahradit s využitím dočasného nebo jiného řešení.

   Maximální doba na odstranění závady se počítá od okamžiku telefonického nahlášení nebo zadání hlášení závady na určené kontakty dodavatele příloha č.4, se zajištěním zpětné vazby o jejím přijetí.
   Do doby na odstranění závady se nezapočítává doba, po kterou jsou dodávány doplňující či upřesňující informace nutné pro řešení.

   Řešení chyb a provozních problémů není omezeno počtem hodin / měsíc.

3. Systémová podpora

3.1 Činnosti vykonávané kontinuálně

- Monitoring událostí – Sběr události z jednotlivých aplikačních a systémových logů SW řešení s cílem identifikovat potencionální problémy s fungováním SW řešení.

3.2 - Činnosti vykonávané alespoň 1x měsíčně
- Kontrola záloh – vlastní proces zálohování provádí Poskytovatel. Kontrola záloh Poskytovatelem spočívá v provedení:
  - kontroly úplnosti záloh,
  - kontroly velikosti zálohovaných dat
  - vytvoření bezpečnostní offline zálohy s periodou 14 dní.

3.3 - Činnosti vykonávané alespoň 1x ročně
- Zálohovací plán – Příprava a aktualizace zálohovacího plánu představuje poskytnutí součinnosti Poskytovatele při aktualizaci zálohovacího plánu pro všechny části SW řešení. Aktualizace zálohovacího plánu spočívá v zajištění těchto činnosti:
  - identifikace datových aktiv (data i SW), stanovení maximální doby ztráty dat, definice zálohovacích postupů.
  - součástí je rovněž součinnost na aktualizaci dokumentace: Zálohovací plán, Recovery plán, Havarijní plán a plán kontinuity služeb, Analýzu rizik.
- Test obnovy – V součinnosti s garantem zálohování Objednatele zajistí Poskytovatel jednou ročně test obnovy SW řešení spočívající v obnově všech části SW řešení (uživatelské rozhraní, aplikační logika a data). Test obnovy spočívá v zajištění těchto činnosti:
  - obnova dat ze záloh,
  - ověření validity dat,
  - ověření funkčnosti integrací,
  - ověření funkčností SW řešení.

VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE
U Nemocnice 499/2, 128 08 Praha 2 | www.vfn.cz, http://intranet.vfn.cz

POUŽÍVÁNÍ SÍTĚ VFN EXTERNÍMI UŽIVATELI

Obsah

Zpracovatel:	**Účinnost dokumentu od:**	**Schválil:**
[redacted]	23. 7. 2020	[redacted]
Garant:	**První vydání dne:**	**Dne:**
[redacted]	1. 1. 2008	23. 7. 2020

POUŽÍVÁNÍ SÍTĚ VFN EXTERNÍMI UŽIVATELI

1 Účel a oblast platnosti dokumentu

Účelem této směrnice je stanovení podmínek pro používání sítě VFN externími uživateli včetně životního cyklu přístupu a povinností, pravidel a restrikcí vztahující se na externí uživatele přistupující do VFN.

2 Pojmy a zkratky

AD	Active Directory
Externí uživatel	Osoba využívající prostředky ICT VFN, která není v pracovně právním poměru k VFN
Garant	Zaměstnanec VFN, který zodpovídá za přístup a práci externího uživatele v síti VFN.
ICT	Informační a komunikační technologie
ISE	Cisco Identity Services Engine
OSICT	Odbor správy ICT
ServiceDesk	Nástroj na zaznamenání, evidenci a sledování stavu incidentů nebo požadavků zaměstnanců VFN a pracovníků externích dodavatelských firem řešených Úsekem informatiky a digitální transformace.
ÚI	Úsek informatiky a digitální transformace
VFN	Všeobecná fakultní nemocnice v Praze
VPN	Virtual Private Network – vzdálený zabezpečený přístup do lokální sítě

3 Odpovědnosti a pravomoci

Garant – zodpovídá za přístup, rozsah oprávnění a práci externího uživatele v síti VFN.

Externí uživatel – externí pracovník, kterému je na základě smluvního vztahu zřízen externí přístup, který je schválen garantem externího přístupu ve VFN (Garant). Výkon práce provádí v souladu se smluvním ujednáním a v souladu s náležitostmi dodržovat povinnosti, pravidla a zákazy uvedené v kap. 4.2.

Pracoviště Dispečinku ÚI (Odbor podpory uživatelů) – zodpovídá za ověření externího uživatele, schválení požadavku Garantem a za zadání požadavku do ServiceDesku.

OSICT – zodpovídá za zpracování a řešení požadavku o VPN přístup.

4 Postup (popis činností)

4.1 PROCESY EXTERNÍHO PŘÍSTUPU

4.1.1 Podmínky schvalování

Externí uživatel musí vyplnit formulář F-VFN-463 Žádost o zřízení přístupu externího uživatele do sítě VFN, kde je uveden garant externího přístupu za VFN (dále jen Garant), na jehož základě dojde k ověření identity žadatele a o schválení validity požadovaného přístupu a rozsahu přístupu Garantem. Po splnění těchto podmínek je možné zřízení účtu externího uživatele.

4.1.2 Postup zřízení přístupu

4.1.2.1 Externí uživatel

Detailní postup pro zřízení účtu externího uživatele je uveden v příloze (Příloha č. 2 – Postup zřízení přístupu externímu uživateli do počítačové sítě VFN) a zároveň dostupný na webové stránce https://www.vfn.cz/externista. Pokud je součástí externího přístupu i požadavek o zřízení vzdáleného přístupu je postupováno dle kapitoly 4.1.2.2 (Vzdálený přístup - VPN). Platnost externího účtu je max. 1 rok od zřízení, pokud nebyl zřizován na dobu určitou. Žadatel bude 1 měsíc před expirací upozorněn na kontaktní e-mail uvedený v žádosti, obdobně i Garant bude upozorněn na svůj pracovní mail 1 měsíc před. O prodloužení přístupového účtu žádá Garant e-mailem – jako odpověď na e-mail s upozorněním na expiraci.

4.1.2.2 Vzdálený přístup - VPN

Externí pracovníci se mohou do sítě VFN připojit pomocí VPN TLS tunelu s multifaktorovou autentizaci. Detailní postup pro žadatele je na stránce https://www.vfn.cz/vpn. O VPN přístup žádá Garant prostřednictvím požadavku do ServiceDesku, kde musí být uvedeno:

- jméno a příjmení externisty,
- účet externisty ve VFN,
- firma,
- telefon,
- e-mail,
- oblast činnosti ve vztahu k VFN,
- na které zařízení (modality, servery) má mít externí uživatel přístup a v jakém rozsahu (IP, porty),
- doba platnosti VPN přístupu, pokud má být na dobu určitou.

Požadavek dále zpracuje pracovník správy sítí OSICT v následujících krocích:

- předá ke schválení vedoucímu OSICT,
- předá na externí firmu Simac, která podle něj nastaví profil v ISE,
- předá na správu serverů OSICT.

Požadavek dále zpracuje pracovník správy serverů OSICT v následujících krocích:

- nastaví profil v AD,
- pošle informace o vytvoření VPN přístupu externímu uživateli,
- ukončí požadavek Garanta v ServiceDesku (čímž dojde k vygenerování a zaslání notifikačního emailu Garantovi).

4.1.3 Zrušení přístupu

Ke zrušení externího účtu nebo VPN přístupu může dojít za následujících podmínek:

- v oprávněných případech, kdy externí uživatel porušil pravidla a povinnosti uvedené v příloze č. 1, Povinnosti při připojování zařízení do sítě VFN,
- pokud je podezření na zavinění bezpečnostního nebo provozního incidentu či byl jakýmkoliv způsobem zapojen do kybernetického útoku na VFN,
- uplynula stanovená doba externího účtu nebo VPN přístupu (výchozí je 1 rok) nebo Garant nepotvrdil prodloužení externího účtu (čímž zanikne i související VPN přístup)
- nebo byl zadán požadavek na zrušení/ukončení externího účtu anebo VPN přístupu,
- požadavek je zpracován pracovníkem OSICT, který odebere členství v odpovídající AD skupině a následně předá na externí firmu Simac, která zruší profil v ISE.

4.2 POVINNOSTI, PRAVIDLA A RESTRIKCE

4.2.1 Povinnosti externích uživatelů

Uživatel v rámci připojení do sítě VFN:

- smí používat připojení pouze k účelům souvisejícím s výkonem smluvní činnosti v takovém rozsahu, který odpovídá potřebám uživatele pro výkon této činnosti,
- je povinen používat své připojení takovým způsobem, který nenaruší funkci sítě, informačních systémů a jejich dat ani práva ostatních uživatelů,
- je povinen chránit svá hesla před vyzrazením a v případě podezření, že heslo zná jiná osoba, heslo musí změnit přes portál http://www.office.com a tuto situaci neprodleně nahlásit jako incident dle bodu 4.2.1.1,
- je povinen zabránit využití či zneužití jeho vzdáleného připojení (VPN) třetí osobou,
- v případě podezření na bezpečnostní incident, nestandardní chování připojení nebo informačních systémů či jakékoliv náznaku na kybernetický útok neprodleně nahlásit toto podezření dle bodu 4.2.1.1,
- je povinen chovat se v souladu s dobrými mravy a právním řádem České republiky.

4.2.1.1 Nahlášení incidentu

V pracovní dny:

- od 7:00 do 16:00 na Dispečink ÚI na tel. [redacted]
- od 16:00 do 7:00 na Pohotovost ÚI na tel. [redacted]

O víkendu a svátcích na Pohotovost ÚI na tel. [redacted]

4.2.2 Požadavky na připojené zařízení

Požadavky a povinnosti vztahující se na zařízení, které je používáno pro externí nebo VPN přístup, jsou uvedeny v příloze č. 1 (Povinnosti při připojování zařízení do sítě VFN) tohoto dokumentu.

4.2.3 Bezpečnostní incident nebo kybernetický útok

V případě bezpečnostní hrozby nebo kybernetického útoku má VFN právo zrušit povolení přístupu externího uživatele anebo VPN přístupu na dobu nezbytnou k analyzování hrozby nebo útoku a zabránění jakéhokoliv ohrožení sítě, informačních systémů a dat VFN. Pokud externí uživatel vykonává nebo má práva správce nebo

administrátora IS VFN, je povinen konat bezodkladně a zajistit dostatek důkazního materiálu dle povinností uvedených v příloze (Příloha č. 3 – Povinnost administrátora v případě bezpečnostního incidentu nebo kybernetického útoku).

4.2.4 Zakázané činnosti

Externí uživatel připojený do sítě VFN nesmí:

- v žádném případě poskytovat informace o přístupu, postupech, přístupová hesla, certifikáty, další citlivé informace a ani jejich části třetím osobám,
- umožnit přístup do sítě jiným osobám (např. umožnit přihlášení pod svým jménem),
- se jakýmkoliv způsobem angažovat při rozesílání a distribuci protiprávních, pomlouvačných, hanlivých, reklamních, agitačních a jiných zpráv,
- v žádném případě předávat jakékoli důvěrné informace získané tímto přístupem třetím osobám (osobní údaje, číselníky, databáze, atd.),
- v síti VFN vyhledávat důvěrné nebo jinak citlivé informace, snažit se získat neautorizovaný přístup k souborům a informacím,
- jakýmkoliv způsobem narušit funkci sítě, informačních systémů a dostupnost jejich dat,
- omezit práva uživatelů/správců ICT nebo získat práva nad rámec svých činností a oprávnění,
- v rámci VFN instalovat nebo ukládat jakýkoli neautorizovaný, nelegální nebo škodlivý software.

4.2.5 Monitoring činností

Veškeré činnosti externího připojení do sítě VFN jsou monitorovány a logovány a pravidelně vyhodnocovány architektem kybernetické bezpečnosti nebo jiným pověřeným zaměstnancem ÚI.

4.2.6 Porušení pravidel a povinností

Externímu uživateli, který poruší pravidla, nedodrží povinnosti nebo provádí zakázané činnosti (viz kap. 4.2):

- bude právo přístupu do sítě VFN neprodleně odebráno,
- porušení může být posuzováno jako závažné porušení povinností vyplývajících z právních předpisů a smluvního vztahu vztahujících se k externímu uživateli vykonávané práci a jednání v rozporu se zájmy VFN a uzavřeného smluvního vztahu.

Externí uživatel připojený do sítě VFN:

- plně zodpovídá za škody vzniklé v důsledku zneužití jeho přístupu zaviněného nedbalostí, nebo poskytnutím přístupu do sítě VFN třetí osobě,
- je plně zodpovědný za obsah svého datového prostoru.

4.3 REVIZE EXTERNÍHO PŘIPOJENÍ

Za oprávněnost, platnost a rozsah externího připojení odpovídá Garant, který v případě jakékoliv změny (zrušení, odebrání/přidání práv, apod.) zadá tuto změnu formou požadavku do ServiceDesku.

V rámci kontrolních mechanizmů je minimálně 1x ročně prováděna kontrola povolených externích uživatelů a připojení VPN v rámci pravidelných auditů KB prováděné auditorem KB nebo jiným pověřeným subjektem.

5 Závěrečná ustanovení

Tato směrnice je závazná pro všechny výše uvedené zaměstnance a externí subjekty v kap. 3 Odpovědnosti a pravomoci.

Porušení této směrnice bude posuzováno jako závažné porušení povinností vyplývajících z právních předpisů a smluvního vztahu vztahujících se k externímu uživateli vykonávané práci a jednání v rozporu se zájmy VFN a uzavřeného smluvního vztahu.

Tato směrnice podléhá revizi nejméně jednou ročně. Za provedení revize dokumentu odpovídá zpracovatel této směrnice.

6 Vznikající dokumenty a údaje

Název	Uchovává	Doba uchování

7 Související dokumenty

RD-VFN-11 Řád používání informačních systémů

F-VFN-463 Formulář: Žádost o zřízení přístupu externího uživatele do sítě VFN

8 Přílohy

Příloha č. 1 – Povinnosti při připojování zařízení do sítě VFN

Příloha č. 2 – Postup zřízení přístupu externímu uživateli do počítačové sítě VFN

Příloha č. 3 – Povinnost administrátora v případě bezpečnostního incidentu nebo kybernetického útoku

POVINNOSTI PŘI PŘIPOJOVÁNÍ ZAŘÍZENÍ DO SÍTĚ VFN

Povinnosti při připojování zařízení do sítě VFN:

1) Připojení každého zařízení do LAN sítě VFN musí být předem konzultováno s Odborem správy ICT Úsekem informatiky a digitální transformace (dále jen ÚI) VFN.
2) Instalace a provozování jakéhokoli software v síti VFN musí být předem konzultováno s Odborem vývoje a správy SW ÚI VFN.
3) Je zakázáno svévolně zapojovat zařízení do LAN sítě a jakkoli měnit LAN síť VFN.
4) Je zakázáno měnit, instalovat a nahrávat jakýkoli softwarový obsah na zařízení VFN.
5) Je zakázáno jakýmkoli způsobem měnit a zasahovat do hardware vybavení VFN.
6) Je zakázáno využívat pro vzdálený přístup na připojovaná zařízení jiných než ÚI VFN schválených metod - viz níže.
7) Při umisťování IT zařízení (server, PC) do sítě VFN je vlastník IT zařízení povinen na své náklady, pokud není ve smlouvě uvedeno jinak, udržovat toto zařízení:
   a. v aktuálním (aktualizace operačního systému, aktualizace antivirového programu)
   b. v bezpečném (nemožnost jednoduše zneužít, používání silných přístupových hesel...) stavu.

   ÚI provádí náhodné testy zneužitelnosti zařízení. V případě zjištění hrozeb nebo nedostatků je vlastník IT zařízení povinen na své náklady zjištěné hrozby a nedostatky neprodleně odstranit.
8) Vlastník IT zařízení je povinen, na vyžádání ÚI, předložit ke kontrole konfiguraci IT zařízení. V situaci, kdy připojené zařízení způsobuje jakékoliv bezpečnostní anebo technické problémy v síti VFN, má VFN možnost takovéto zařízení bez předchozího upozornění odpojit od sítě VFN a externí účet (včetně VPN připojení) zablokovat nebo i zrušit.

Případné dotazy, požadavky nebo problémy je možné řešit na:

- od 7:00 do 16:00 Dispečink ÚI na tel. +[redacted]

Metoda vzdáleného přístupu

K připojovaným zařízením je možné, pokud tomu nebrání další důvody, zřídit vzdálený přístup typu VPN připojení (IPSec tunel nebo jeho obdoba). Je nutná instalace Cisco VPN klienta.

Info: https://www.vfn.cz/vpn nebo Pohotovosti ÚI: [redacted](mimo pracovní hodiny Dispečinku ÚI).

POSTUP ZŘÍZENÍ PŘÍSTUPU EXTERNÍMU UŽIVATELI DO POČÍTAČOVÉ SÍTĚ VFN

Postup

Postup žádosti o povolení přístupu do počítačové sítě VFN:

- Žadatel si stáhne, vytiskne a vyplní formulář F-VFN-463.
- Žadatel se dostaví s vyplněným a NEPODEPSANÝM formulářem na Dispečink Úseku informatiky a digitální transformace (dále jen Dispečink ÚI) ve VFN (Budova ředitelství A5, pracovní dny 7:00 – 16:00).
- Pracovník Dispečinku ÚI ověří identitu žadatele (OP, pas). Žadatel podepíše formulář.
- Pracovník Dispečinku ÚI zašle na uvedeného Garanta e-mail s žádostí o schválení validity požadovaného přístupu a rozsahu přístupu. V případě požadavku na VPN připojení, je Garant upozorněn.
- Po obdržení potvrzení od Garanta bude vytvořen přístupový účet externího uživatele a případně VPN přístup.
- Žadatel bude o schválení a zřízení přístupového účtu informován e-mailem.
- Žadatel se dostaví na Dispečink ÚI a vyzvedne si uživatelské jméno a heslo. Heslo je doporučeno si na místě změnit.
- Expirace přístupového účtu je max. po 1 roce od zřízení. Žadatel i Garant bude 1 měsíc před expirací upozorněn na zadaný e-mail. O prodloužení přístupového účtu žádá Garant e-mailem – jako odpověď na e-mail s upozorněním na expiraci.

Upozornění: *Přístup do počítačové sítě VFN se nezřizuje na počkání!*

Povinnosti, pravidla a omezení

Po dobu platnosti účtu externího uživatele je externí uživatel povinen dodržovat následující:

- stanovené povinnosti, pravidla a případné restrikce v kap. 4.2 Řádu používání sítě VFN externími uživateli (SM-UI-02),
- při používání VPN přístupu:
  - stanovené povinnosti pro připojování zařízení do sítě VFN definované v příloze č. 1 (SM-UI-02),
  - návody a postupy pro VPN připojení do sítě VFN uvedené na webových stránkách https://www.vfn.cz/vpn,
- aktuální informace uvedená na webových stránkách https://www.vfn.cz/externista.

Dokumenty ke stažení

- Formulář F-VFN-463 Žádost o zřízení přístupu externího uživatele do sítě VFN
- Řád používání sítě VFN externími uživateli (SM-UI-02)

Kontakt

Dispečink ÚI

- Všeobecná fakultní nemocnice v Praze, U Nemocnice 499/2, 128 08 Praha 2
- Telefon: [redacted]
- E-mail: [redacted]

POVINNOST ADMINISTRÁTORA V PŘÍPADĚ BEZPEČNOSTNÍHO INCIDENTU NEBO KYBERNETICKÉHO ÚTOKU

Povinnosti administrátora

V případě podezření či probíhajícím bezpečnostním incidentu nebo kybernetickém útoku je povinností správce nebo administrátora konat bezodkladně a zajistit dostatek důkazního materiálu:

- k identifikaci zdroje nebo příčiny,
- k čemu došlo nebo jak se projevuje,
- důsledkům a možným dopadům,

u tohoto incidentu či útoku je vždy povinen:

- zajistit kopie logů nebo transakčních záznamů, pokud by to nezpůsobilo jejich poškození nebo smazání,
- iniciovat nebo pozastavit šíření či poškození, zamezit incidentu nebo útoku,
- nemazat jakákoliv data o kybernetickém bezpečnostním incidentu bez svolení VFN, Policie ČR nebo NÚKIB,
- nahlásit toto podezření neodkladně na Pohotovost ÚI jako bezpečnostní nebo kybernetický incident:
    - v pracovní dny:
        - od 7:00 do 16:00 na Dispečink ÚI na tel. [redacted]
        - od 16:00 do 7:00 na Pohotovost ÚI na tel. [redacted]
    - o víkendu a svátcích na Pohotovost ÚI na tel. [redacted]

Příloha č. 4

Seznam oprávněných osob

A. Seznam kontaktních osob Poskytovatele oprávněných poskytovat podporu.

Jméno	Funkce	E-mail	Telefonní číslo
	Helpdesk	[redacted]	[redacted]
[redacted]	Senior consultant	[redacted]	[redacted]

B. Seznam kontaktních osob Objednatele oprávněných k hlášení požadavků na poskytování podpory.

Jméno	Funkce	E-mail	Telefonní číslo
	Dispečink ÚIDT	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

C. Seznam kontaktních osob Objednatele určených k hlášení oznámení, požadavků, událostí nebo incidentů Poskytovatele ve vztahu k ochraně osobních údajů nebo bezpečnosti informací nebo kybernetické bezpečnosti.

Oblast	Funkce	Kontakt
Ochrana osobních údajů	Pověřenec pro ochranu osobních údajů	[redacted]
Bezpečnosti informací, kybernetické bezpečnost	Manažer kybernetické bezpečnosti	[redacted]

Příloha č. 5

Požadavky systému řízení bezpečnosti informací na dodavatele

1 Účel

Účelem toho dokumentu je stanovit požadavky vyplývající ze systému řízení bezpečnosti informací ve VFN pro dodavatele jako provozovatele, Poskytovatele služeb nebo zajišťující podporu základních služeb: zdravotních služeb dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen ZKB).

Příloha vymezuje obecná pravidla a zásady kybernetické bezpečnosti vztahující se na smluvní plnění dodavatele, pokud nejsou detailně specifikovány Smlouvou. Tato příloha nerozšiřuje předmět plnění dodavatele vymezený smlouvou, ale pouze specifikuje relevantní požadavky systému řízení bezpečnosti informací ve VFN, které musí dodavatel při plnění dodržovat.

Dodavatel je povinen prokazatelně seznámit všechny své zainteresované zaměstnance s obsahem tohoto dokumentu.

2 Bezpečnostní požadavky

Dodavatel ve vztahu k předmětu plnění smlouvy musí definovat v interních předpisech, konfiguračních a instalačních manuálech, postupech nebo jiných dokumentech sloužících k předmětu dodávané služby či musí plnit zde popsané povinnosti.

Obecná pravidla bezpečnosti informací

Dodavatel je povinen:

- vydefinovat rozsah prací/služeb/podpory v kompetenci dodavatele a podmínky spolupráce mezi smluvními stranami,
- specifikovat popis používání každé služby provozované nebo spravované dodavatelem,
- stanovit cílové úrovně služby a neakceptovatelné nebo zakázané úrovně služby,
- vést seznam jednotlivců, kteří vzhledem ke svým předdefinovaným právům a privilegiím jsou oprávněni zajišťovat smluvní služby,
- umožnit VFN právo monitorovat nebo auditovat smluvní povinnosti i u dodavatele,
- stanovit popis eskalace problému v případech řešení havárie s popisem pravidel pro řešení havarijních situací,
- zajistit školení zainteresovaných uživatelů a správců dodavatele v metodách, postupech a v bezpečnosti,
- upřesnit podmínky spolupráce dodavatele se subdodavateli (třetí stranou),
- informovat Objednatele o způsobu řízení rizik a o zbytkových rizicích,
- informovat o významné změně dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, či ekvivalentním postavení, nebo o změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy,
- provést neprodlené nahlášení identifikovaných bezpečnostních událostí a slabin kontaktní osobě za VFN.

Fyzická bezpečnost

Dodavatel je povinen:

- nastavit komplexní opatření fyzické bezpečnosti v prostředí dodavatele, jež zabrání nebo sníží pravděpodobnost vzniku ohrožení IS základní služby, ztrát dat a jiného duševního vlastnictví, přerušení činností či poškozování jiných důležitých zájmů VFN,
- dodržovat režimová nebo organizační opatření VFN při vjezdu do objektů nebo vstupu do prostor nebo překonávání fyzických/logických zábran těchto objektů nebo prostor VFN,
- dobrovolně se podrobit případným kontrolám vnášených/vynášených osobních věcí nebo jakýchkoliv předmětů při vstupu nebo odchodu z objektů nebo prostor VFN prováděné oprávněnými zaměstnanci VFN (ostraha, vrátný, recepce apod.),
- neprovádět fotografování, video/audio záznam nebo kopírování/scanování dokumentů bez souhlasu oprávněného zaměstnance VFN. V prostorách kategorie zóny „C" (např. serverovna) pouze na základě písemného povolení vedení VFN.

Bezpečnost lidských zdrojů

Dodavatel je povinen:

- prokazatelně seznámit zaměstnance dodavatele s dodržováním bezpečnostních pravidel a zásad požadovaných VFN,
- dodržovat ochranu aktiv VFN před neautorizovaným přístupem, vyzrazením, modifikací, zničením nebo narušením,

- zachovávat mlčenlivost o důvěrných údajích nebo sděleních VFN a o jejich ochraně,
- stanovit odpovědnosti zaměstnanců dodavatele pro nakládání s informacemi,
- poučit zaměstnance dodavatele hlásit zjištěné bezpečnostní události nebo jiná bezpečnostní rizika odpovědné osobě dodavatele,
- provádět pravidelné školení zaměstnanců dodavatele v souvislosti s bezpečností informací,
- při porušení pracovních povinnosti zaměstnance dodavatele ve vztahu k bezpečnosti informací nebo způsobení bezpečnostního incidentu, musí být zahájeno formální disciplinární řízení. Způsob řízení odpovídá povaze porušení nebo incidentu a jeho dopadu na VFN.

Řízení přístupu

Dodavatel je povinen:

- dodržovat princip minimálních oprávnění: přidělovat oprávnění na nejnižší možné úrovni, která umožní jejich správnou funkci,
- dodržovat požadavky na řízení přístupu:
    - definovat procesy přidělování, správy oprávnění, pravidelně provádět audit přidělených oprávnění a odstraňovat účty při odchodu zaměstnance nebo změně jeho zařazení,
    - přidělovat privilegovaná oprávnění takovým způsobem, aby byla zajištěna jednoznačná auditovatelnost všech kroků provedených pod těmito účty ve vztahu ke konkrétním osobám.

Bezpečné chování uživatelů

Uvedené povinnosti se vztahují na prostředí VFN nebo zařízení používané ke správě nebo administraci předmětu smlouvy.

Zaměstnanec dodavatele:

- nesmí šířit a vědomě používat SW získaný v rozporu s právními předpisy, zejména s autorským zákonem a SW, získaný v souladu s těmito předpisy nesmí užívat v rozporu se smlouvou,
- musí používat počítačové prostředky a SW vybavení VFN jen v rámci smluvního ujednání a stanovené kompetence,
- je povinen respektovat pravidla tvorby a nakládání s přístupovými hesly definovaná VFN,
- je povinen zachovávat důvěrnost hesel jemu přidělených v rámci své kompetence,
- nesmí žádnými prostředky se pokusit získat přístupová práva či privilegovaný stav, který mu nebyl přidělen,
- nesmí se pokusit získat přístup k chráněným informacím a datům jiných uživatelů nebo systémů,
- musí dodržovat předepsaná opatření pro užití prostředků pro vzdálený přístup (aktualizace systému, spuštěný FW a antivir, využití veřejných sítí apod.).

Bezpečnost mobilních zařízení a vzdáleného přístupu

Přístup externích zařízení do prostředí Objednatele je možný po provedení registrace zařízení při dodržení postupu „Přístup do počítačové sítě VFN pro externí zaměstnance/firmy", zde uvedených povinností a směrnice Používání sítě VFN externími uživateli (SM-UI-02). Uživatel dodavatele připojený do sítě VFN je povinen:

- používat je pouze k účelům a po dobu souvisejícím s výkonem smluvní činnosti v takovém rozsahu, který odpovídá potřebám uživatele pro výkon této činnosti,
- používat své připojení takovým způsobem, který nenaruší funkci sítě ani práva ostatních uživatelů,
- chránit svá hesla před vyzrazením, a v případě podezření, že heslo zná jiná osoba, tuto situaci neprodleně nahlásit Poskytovateli připojení,
- zabránit využití či zneužití jeho vzdáleného připojení třetí osobou,
- chovat se v souladu s dobrými mravy a právním řádem České republiky.

Ochrana před škodlivým kódem

Ve vztahu k dodavatelským pracím a službám zajišťujícím provoz a fungování základních služeb VFN musí být zajištěna ochrana vnějšího perimetru dodavatele, komunikace, IS, úložišť a koncových stanic nebo mobilních zařízení před škodlivým kódem.

Zálohování a obnova dat

Dodavatel je povinen provádět zálohování dat a informací v provozovaných nebo spravovaných HW, IS a jejich datech k zajištění jejich dostupnosti v případě nestandardních událostí (chyba paměťového média, havárie systému, poškození integrity dat atp.), aby bylo možné zálohovaná data použít pro jejich obnovu nebo přesun do jiného prostředí.

Zálohovaná data musí splňovat požadavky:

- na kompletní obnovu dat,

- dodržet maximálně tolerovaný prostoj (MTD) definovaný ve smlouvě,
- pravidelné provádění záloh a testování jejich obnovy,
- zajištění ochrany záloh a obsažených dat včetně jejich integrity,
- vydefinovaná správa (včetně řízení přístupu), doba uchování, cykly a počet kopií zálohovaných dat.

Technické zranitelnosti

Dodavatel je povinen:

- identifikovat a odstraňovat technické zranitelnosti spojené s bezpečnostním nastavením nebo fungováním jím provozovaných/spravovaných zařízení nebo systémů,
- upozorňovat VFN na identifikované zranitelnosti zařízení nebo systémů ve správě VFN nebo subdodavatelů,
- provádět ověření/testování opravy zranitelnosti v testovacím nebo integračním prostředí před instalací opravy programového vybavení do produkčního prostředí.

Bezpečnost komunikační sítě

Dodavatel je povinen omezit riziko napadení systémů nebo služeb prostřednictvím počítačové sítě, např. využitím:

- šifrování,
- řízené kontroly přístupu,
- zamezením napadení aktivním útočníkem,
- řízením zátěže,
- zajištěním integrity dat,
- samostatné lokální sítě,
- víceúrovňovou bezpečností,
- využitím vhodné sítě.

Bezpečnostní zásady pro práci s daty

Dodavatel je povinen:

- dodržovat stanovená pravidla ochrany dat zahrnující speciální nakládání s tajnými, důvěrnými, osobními a citlivými údaji dle jednotlivých zákonů (např. nařízení č. 2016/679 - GDPR, zákona č. 110/2019 Sb., zákon č. 412/2005 Sb. apod.),
- zajistit řízení přístupu k datům s využitím principu minimálních oprávnění,
- ochránit data při přenosu, předání a v datovém úložišti,
- plnit povinnosti ochrany osobních údajů, a to především technická nebo organizační opatření, hlášení úniku osobních údajů, spolupráce na řešení incidentů nebo auditu ochrany osobních údajů apod.,
- dodržet závazek dodavatele (a subdodavatele) neporušovat integritu a dostupnost aktiv,
- stanovit omezení platná pro kopírování a šíření informací,
- přijmout opatření zajišťující vrácení či zničení informací po ukončení smluvního vztahu nebo v jeho průběhu,
- definovat postupy bezpečné likvidace dat.

Používání kryptografické ochrany

Dodavatel je povinen:

- využívat úrovně ochrany s ohledem na typ a sílu kryptografického algoritmu ve vztahu k citlivosti jednotlivých informačních aktiv,
- zohledňovat známá nebo odhalená rizika a zranitelnosti pro použité typy a síly kryptografických algoritmů výměnou za „bezpečné" (neprolomené) kryptografické algoritmy.

Akvizice, vývoj a údržba informačních systémů

Dodavatel je povinen:

- dodržovat bezpečnostní pravidla, noremy a best practices (např. OWASP - Open Web Application Security Project) v rámci celého životního cyklu nákupu a vývoje SW od zadání, návrhu, přes vývoj a testování až po nasazení do provozu,
- zavést oddělení rolí vývoje, testu a provozu; vytvářet a provozovat vývojové, integrační, testovací a provozní prostředí tak, aby byla zcela oddělena v sítích a byla podporována oddělenými stroji,

- zohlednit bezpečnostní požadavky VFN na dodávaný nebo vyvíjený SW, a to především:
    - podporované frameworky a platformy v prostředí VFN,
    - nefunkční bezpečnostní požadavky,
    - provádět ověření codereview v jednotlivých fázích vývoje a testování,
    - spolupracovat na bezpečnostním testování včetně penetračních testů,
    - dodávat systémové a provozní bezpečnostní dokumentace,
- stanovit způsob převzetí, akceptace a instalaci do produkčního prostředí,
- používat jasný a specifikovaný proces řízení změn.

Zvládání bezpečnostních incidentů

Dodavatel je povinen:

- mít ve svém prostředí zavedený systém hlášení, upozorňování a vyšetřování bezpečnostních nebo kybernetických incidentů a případů prolomení bezpečnosti,
- neprodleně oznámit Objednateli bezpečnostní nebo kybernetický incidenty a prolomení bezpečnosti v prostředí dodavatele nebo Objednatele,
- spolupracovat s Objednatelem na vyšetření, vyhodnocení a přijetí opatření z bezpečnostního nebo kybernetického incidentu v prostředí Objednatele.

Řízení kontinuity činností

Dodavatel je povinen:

- vytvořit takové postupy a fungující prostředí, které umožní zajistit kontinuitu a obnovu klíčových procesů a činností základních služeb VFN provozovaných nebo spravovaných dodavatelem HW, IS a jejich dat v případě jejich narušení nebo ztráty,
- provádět pravidelné testování, vyhodnocování a případně aktualizování havarijních plánů obnovy (DRP).

Legislativní a normativní požadavky

Dodavatel je povinen splnit legislativní a normativní požadavky:

- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a vyhlášku č. 82/2018Sb., o kybernetické bezpečnosti,
- nařízení EU č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR),
- zákon č. 110/2019 Sb., zpracování osobních údajů,
- směrnici EU č. 2016/1148, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů (NIS),
- nařízení EU č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS),
- standardy systému řízení bezpečnosti řady ISO/IEC 27000 – Information Security Management System (ISMS), především ISO/IEC 27001, ISO/IEC 27002 a ISO/IEC 27799,
- a související normy nebo best-practice.

Kontroly zavedení bezpečnostních opatření

Dodavatel je povinen provádět kontroly zavedených bezpečnostních opatření v prostředí dodavatele v pravidelných intervalech a následně přijímat odpovídající preventivní nebo systémová nebo organizační opatření na zjištěné nedostatky nebo zranitelnosti a umožnit VFN ověření provádění kontrol a aplikaci následných opatření.

Audity plnění bezpečnostních požadavků

Dodavatel je povinen umožnit VFN provedení auditu plnění požadavků uvedených v tomto dokumentu nebo s kterými byl prokazatelně Dodavatel seznámen, a to po předchozím upozornění. Audit bude proveden zaměstnanci VFN nebo jím smluvně pověřeným subjektem.

Příloha č. 6

Průběh inflace

	Tabulka průběhu inflačního navýšení ceny podle			
	smlouvy č. 177/2005 ze dne 4.dubna 2005			
rok	cena základ	inflace ČSÚ	navýšení	celkem
	Kč	%	Kč	Kč
2005	604 440,00	0	0,00	604 440,00
2006	604 440,00	1,9	11 484,36	615 924,36
2007	615 924,36	2,5	15 398,11	631 322,47
2008	631 322,47	2,8	17 677,03	648 999,50
2009	648 999,50	6,3	40 886,97	689 886,47
2010	689 886,47	1	6 898,86	696 785,33
2011	696 785,33	1,5	10 451,78	707 237,11
2012	707 237,11	1,9	13 437,51	720 674,62
2013	720 674,62	3,3	23 782,26	744 456,88
2014	744 456,88	1,4	10 422,40	754 879,28
2015	754 879,28	0,4	3 019,52	757 898,79
2016	757 898,79	0,3	2 273,70	760 172,59
2017	760 172,59	0,7	5 321,21	765 493,80
2018	765 493,80	2,5	19 137,34	784 631,14
2019	760 172,59	0	0,00	760 172,59
2020	760 172,59	0	0,00	760 172,59
2021	760 172,59	0	0,00	760 172,59
2022	760 172,59	0	0,00	760 172,59
2023	*760 172,59*	*15,1*	*114 786,06*	***874 958,65***