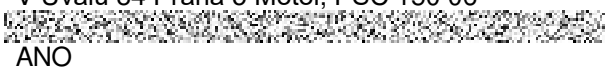
Servisní smlouva č. 2303100318

na nemocniční informační systém – moduly pracovišť komplementu

SMLUVNÍ STRANY

Objednatel

Fakultní nemocnice v Motole
IČO: 00064203
DIČ: CZ00064203
se sídlem: V Úvalu 84 Praha 5 Motol, PSČ 150 06
zastoupený: 
plátce DPH: ANO
bankovní spojení (číslo účtu): 17937051/0710
telefon: 
e-mail:
ID datové schránky: nk8bxj3

(dále jen „***Objednatel***“)

a

Poskytovatel

Steiner, s.r.o.
IČO: 26488931
DIČ: CZ26488931
se sídlem: Jevanská 2423/10, Strašnice, 100 00 Praha 10
zastoupený: 
plátce DPH: ANO
zapsaný v obchodním rejstříku vedeném u Městského soudu v Praze pod sp. zn. C 85437
bankovní spojení (číslo účtu): 
telefon:
e-mail:
ID datové schránky: nba4qm3

(dále jen „***Poskytovatel***“)

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

uzavřeli v souladu s § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „***Občanský zákoník***“), tuto servisní smlouvu (dále jen „***Smlouva***“).

I. ÚVODNÍ UJEDNÁNÍ

1. Smlouva je uzavřena na základě výsledků zadávacího řízení (dále jen „***Řízení veřejné zakázky***“) veřejné zakázky s názvem: **„FN Motol – Servis Nemocničního informačního systému“**, ev. č. zakázky ve Věstníku veřejných zakázek: **Z2023-010562** (dále jen „***Veřejná zakázka***“). Jednotlivá ujednání Smlouvy tak budou vykládána v souladu se zadávacími podmínkami Veřejné zakázky a nabídkou Poskytovatele podanou na Veřejnou zakázku.

2. Objednatel naplňuje požadavky vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, a proto byl Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) určen v souladu s § 22a zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „***zákon o kybernetické bezpečnosti***“), za správce a provozovatele systému základní služby. Objednatel je tak povinen zohlednit požadavky vyplývající z bezpečnostních opatření v Řízení veřejné zakázky a tyto požadavky zahrnout do této Smlouvy.

3. Objednatel je správcem a provozovatelem informačního systému základní služby, proto poskytnutí níže specifikovaných služeb musí splňovat podmínky zákona o kybernetické bezpečnosti a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „***vyhláška o kybernetické bezpečnosti***“).

4. Objednatel upozorňuje, že podle § 2 písm. n) a podle § 8 odst. 1 písm. b) vyhlášky o kybernetické bezpečnosti bude evidovat Poskytovatele jako svého významného dodavatele a bude požadovat plnění povinností vyplývajících z vyhlášky o kybernetické bezpečnosti. Poskytovatel bere na vědomí, že bude Objednatelem veden v jeho evidenci významných dodavatelů. Poskytovatel prohlašuje, že se s povinnostmi vyplývajícími z vyhlášky o kybernetické bezpečnosti seznámil a zavazuje se k jejich plnění.

5. Poskytovatel je povinen při plnění Smlouvy zajistit dodržování požadavků na kybernetickou bezpečnost a prohlašuje, že při své činnosti postupuje v souladu se zákonem o kybernetické bezpečnosti a vyhláškou o kybernetické bezpečnosti.

II. ÚČEL SMLOUVY

1. Účelem této Smlouvy je zajištění maintenance, podpory provozu, servisu a rozvoje nemocničního informačního systému – moduly pracovišť komplementu (dále „**Systém**“) Poskytovatelem pro Objednatele tak, aby byla zajištěna maximální možná funkčnost Systému, a to plně v souladu s požadavky stanovenými v této Smlouvě, případně v jejích přílohách. Za Systém jsou ve smyslu této Smlouvy považovány také jednotlivé moduly pracovišť komplementu.

2. Pro vyloučení jakýchkoliv pochybností Smluvní strany uvádějí, že v případě jakékoliv nejistoty ohledně výkladu ustanovení této Smlouvy budou tato ustanovení vykládána tak, aby v co nejširší míře zohledňovala účel této Smlouvy.

III. PŘEDMĚT SMLOUVY

1. Předmětem Smlouvy je závazek Poskytovatele zajišťovat maintenance, podporu provozu, servis, rozvoj Systému a poskytování dalších služeb za podmínek uvedených v této Smlouvě a závazek Objednatele řádně a včas poskytnuté služby převzít a uhradit za ně Poskytovateli sjednanou cenu dle této Smlouvy.

2. Služby maintenance a podpory provozu a servisu Systému (dále jen „***Průběžně poskytované Služby***“) budou spočívat zejména v:

   2.1. zajištění dostupnosti Systému odstraňováním jeho chyb (vad) bez ohledu na jejich původ (Odstraňování vad Systému);

   2.2. poskytování služby online helpdeskového systému, telefonické hotline a e-mailu (Technická podpora);

   2.3. zajištění 2. a 3. úroveň podpory (L2 / L3) pro databázi a všechny aplikační nástroje;

   2.4. pravidelné profylaktické kontroly Systému, aplikací a databází;

2.5. zajištění upgrade/update Systému a technologické a legislativní aktualizace Systému;

2.6. podpoře uživatelů při obsluze a užívání Systému, zejména zodpovídáním telefonických a e-mailových dotazů oprávněných uživatelů Systému, podáváním technických informací o Systému a v poskytování asistence oprávněným uživatelům prostřednictvím vzdáleného přístupu;

2.7. provedení čtvrtletní rozvojové schůzky;

2.8. poskytování dalších plnění dle této Smlouvy či jejích příloh.

Bližší podmínky Průběžně poskytovaných Služeb jsou uvedeny v příloze Smlouvy (Příloha č. 1 Smlouvy).

Popis současného stavu Systému ke dni nabytí účinnosti Smlouvy je uveden v příloze Smlouvy (Příloha č. 2 Smlouvy).

3. Služby rozvoje Systému (dále jen „***Služby na objednávku***“) bude Poskytovatel poskytovat vždy na základě dílčích objednávek Objednatele dle aktuálních potřeb a pokynů Objednatele. V rámci Služeb na objednávku bude kromě rozvoje Systému poskytováno rovněž napojování nových analyzátorů Objednatele na Systém, školení dle potřeb Objednatele, případně další služby požadované Objednatelem, jako například konzultace, služby konfigurace a nastavení Systému apod.

4. Průběžně poskytované Služby a Služby na objednávku společně dále jen „***Služby***“.

IV. CENA SLUŽEB

1. Cena Služeb (dále jen „***Cena Služeb***“) je upravena následovně:

1.1. Cena Průběžně poskytovaných Služeb je uvedena v Ceníku Služeb (Příloha č. 3 Smlouvy). Cena Průběžně poskytovaných Služeb je členěna dle jednotlivých modulů pracovišť komplementu.

1.2. Cena Služeb na objednávku je uvedena v Ceníku Služeb (Příloha č. 3 Smlouvy). Cena Služeb na objednávku je členěna dle jednotlivých druhů Služeb na objednávku.

2. V Ceně Služeb je zahrnut zisk Poskytovatele a veškeré náklady, jež mohou Poskytovateli v souvislosti s poskytováním Služeb vzniknout, zejména cestovní výdaje, cena softwarového a hardwarového vybavení a licencí.

V. FAKTURACE A PLATEBNÍ PODMÍNKY

1. Je-li Poskytovatel povinen podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen ***„ZoDPH“***) uhradit v souvislosti s poskytováním plnění podle Smlouvy DPH a poskytnuté Služby nepodléhají režimu přenesení daňové povinnosti dle ZoDPH, je Objednatel povinen Poskytovateli takovou DPH uhradit vedle Ceny Služeb. Poskytovatel odpovídá za to, že sazba DPH bude ve vztahu ke všem plněním poskytovaným na základě Smlouvy stanovena v souladu s právními předpisy platnými a účinnými k okamžiku uskutečnění zdanitelného plnění.

2. Objednatel uhradí Poskytovateli Cenu Služeb na základě jednotlivých faktur (dále jen „***Faktura***“), vystavených dle následujících odstavců.

3. Cena Průběžně poskytovaných Služeb bude zaplacena vždy po skončení kalendářního měsíce, ve kterém byly příslušné Průběžně poskytované Služby poskytovány, a to na základě faktury vystavené Poskytovatelem. Poskytovatel se zavazuje fakturu vystavit nejpozději do 5 pracovních dnů od schválení příslušného Dílčího měsíčního výkazu Objednatelem dle čl. VII. odst. 4. této Smlouvy. Přílohou faktury musí být kopie Objednatelem schváleného Dílčího měsíčního výkazu poskytnutých služeb. V případě, že příslušné Průběžně poskytované Služby nebyly poskytovány po celý kalendářní měsíc, náleží Poskytovateli alikvotní část měsíční ceny příslušných Průběžně poskytovaných Služeb. Faktura bude zohledňovat členění ceny Průběžně poskytovaných Služeb dle jednotlivých modulů pracovišť komplementu stanovené v Ceníku Služeb (Příloha č. 3 Smlouvy).

4. Cena Služeb na objednávku bude Objednatelem uhrazena vždy zpětně, a to na základě faktury vystavené Poskytovatelem. Poskytovatel se zavazuje fakturu vystavit nejpozději do 5 pracovních dnů od akceptace výsledku Služby na objednávku ze strany Objednatele

postupem dle článku VIII této Smlouvy. Přílohou faktury musí být kopie protokolu schváleného Objednatelem ve vztahu ke Službě na objednávku, ke kterému je faktura vystavována.

5. Faktura musí splňovat náležitosti daňového dokladu podle ZoDPH, včetně případné informace, že poskytování Služeb podléhá režimu přenesení daňové povinnosti dle ZoDPH. V případě, že Poskytovatel není plátcem DPH, musí Faktura splňovat náležitosti účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů. Faktura musí vždy splňovat náležitosti stanovené § 435 Občanského zákoníku. Poskytovatel je povinen použít na Faktuře bankovní účet zveřejněný v registru plátců podle § 96 ZoDPH.

6. Splatnost Faktury činí 60 dnů ode dne doručení Faktury Objednateli.

7. Stanoví-li Faktura splatnost delší, než je jako minimální stanovena v tomto článku, je Objednatel oprávněn uhradit Cenu Služeb a případnou DPH ve lhůtě splatnosti určené ve Faktuře.

8. Cena Služeb vyúčtovaná Fakturou a případná DPH je uhrazena vždy dnem jejich odepsání z bankovního účtu Objednatele.

9. Objednatel si vyhrazuje právo uplatnit institut zvláštního způsobu zajištění daně z přidané hodnoty ve smyslu § 109a ZoDPH, pokud Poskytovatel bude požadovat úhradu za zdanitelné plnění na bankovní účet, který nebude nejpozději ke dni splatnosti příslušné Faktury zveřejněn správcem daně v příslušném registru plátců daně (tj. způsobem umožňujícím dálkový přístup). Obdobný postup je Objednatel oprávněn uplatnit i v případě, že v okamžiku uskutečnění zdanitelného plnění bude o Poskytovateli zveřejněna v příslušném registru plátců daně skutečnost, že je nespolehlivým plátcem nebo v případě naplnění dalších kritérií uvedených v § 109 odstavci 1 a 2 ZoDPH. V případě, že nastanou okolnosti umožňující Objednateli uplatnit zvláštní způsob zajištění daně podle § 109a ZoDPH, bude Objednatel o této skutečnosti Poskytovatele informovat. Při použití zvláštního způsobu zajištění daně bude příslušná výše DPH zaplacena na účet Poskytovatele vedený u jeho místně příslušného správce daně, a to v původním termínu splatnosti. V případě, že Objednatel institut zvláštního způsobu zajištění daně z přidané hodnoty ve shodě s tímto ujednáním uplatní, a zaplatí částku odpovídající výši daně z přidané hodnoty uvedené na daňovém dokladu vystaveném Poskytovatelem na účet Poskytovatele vedený u jeho místně příslušného správce daně, bude tato úhrada považována za splnění části závazku Objednatele odpovídajícího příslušné výši DPH, kterou je povinen dle Smlouvy uhradit vedle Ceny Služeb.

10. Nebude-li příslušná Faktura obsahovat některou povinnou nebo dohodnutou náležitost nebo bude-li chybně stanovena Cena Služeb, DPH nebo jiná náležitost Faktury, je Objednatel oprávněn tuto Fakturu vrátit Poskytovateli k provedení opravy s vyznačením důvodu vrácení. Poskytovatel je povinen opravit Fakturu podle pokynů Objednatele a opravenou Fakturu neprodleně doručit Objednateli. Splatnost opravené faktury činí 30 dnů ode dne doručení Faktury Objednateli, čl. V. odst. 7 Smlouvy se použije obdobně.

11. Objednatel neposkytuje Poskytovateli žádné zálohy.

VI. MÍSTO A DOBA PLNĚNÍ

1. Místem plnění je sídlo Objednatele a dále jakékoli další pracoviště Objednatele dle jeho písemného pokynu. Pokud to povaha plnění této Smlouvy umožňuje a Objednatel vůči tomu nemá výhrady, je Poskytovatel oprávněn poskytovat Služby vzdáleným přístupem, zejména prostřednictvím služby helpdesk.

2. Poskytování Průběžně poskytovaných Služeb bude zahájeno na základě písemné výzvy Objednatele doručené Poskytovateli (dále jen „***Výzva k zahájení poskytování Průběžně poskytovaných Služeb***“) a bude poskytováno nepřetržitě po dobu účinnosti této Smlouvy. Poskytovatel je povinen zahájit poskytování Průběžně poskytovaných Služeb od data uvedeného ve Výzvě k zahájení poskytování Průběžně poskytovaných Služeb, byla-li Výzva k zahájení poskytování Průběžně poskytovaných Služeb Poskytovateli doručena včas, nebo oznámí-li Poskytovatel písemně Objednateli, že na včasném doručení Výzvy k zahájení poskytování Průběžně poskytovaných Služeb netrvá. Výzva k zahájení poskytování Průběžně poskytovaných Služeb byla doručena včas, byla-li Poskytovateli Objednatelem doručena alespoň 14 dní před datem stanoveného zahájení poskytování Průběžně poskytovaných Služeb uvedeným ve Výzvě k zahájení poskytování Průběžně poskytovaných Služeb. Objednatel odešle Výzvu k zahájení poskytování Průběžně poskytovaných Služeb nejpozději do 4 měsíců ode dne nabytí účinnosti této Smlouvy. Pokud Objednatel neodešle Výzvu k zahájení poskytování Průběžně poskytovaných Služeb ani do 1 roku ode dne nabytí účinnosti této Smlouvy, je Poskytovatel oprávněn od této Smlouvy odstoupit.

3. Služby na objednávku budou poskytovány dle podmínek stanovených v článku VIII této Smlouvy.

VII. POSKYTOVÁNÍ PRŮBĚŽNĚ POSKYTOVANÝCH SLUŽEB

1. Vznikne-li při poskytování Služeb Poskytovatelem výstup, k němuž bude možné a účelné poskytovat Průběžně poskytované Služby, zavazuje se Poskytovatel zahájit poskytování Průběžně poskytovaných Služeb k takovýmto výstupům ode dne jejich akceptace. Tento odstavec Smlouvy se tak mimo jiné vztahuje na výsledky Služeb na objednávku, přičemž Cena Průběžně poskytovaných Služeb se nemění.
2. Poskytovatel se zavazuje poskytovat Průběžně poskytované Služby v kvalitě definované v jednotlivých Service Level Agreements (dále jen „***SLA***“), které jsou součástí Příloha č. 1 této Smlouvy.
3. Poskytovatel je povinen vypracovávat a Objednateli doručovat přehledné a kompletní výkazy a výsledky poskytování Průběžně poskytovaných Služeb (dále jen „***Dílčí měsíční výkaz***“), ze kterých bude jednoznačně zřejmé, zda byly Průběžně poskytované Služby poskytovány v kvalitě definované dle jednotlivých SLA dle této Smlouvy, resp. její přílohy (Příloha č. 1 Smlouvy).
4. Dílčí měsíční výkazy budou vypracovávány vždy pro vyhodnocovací období 1 kalendářního měsíce (dále jen „***Vyhodnocovací období***“) a budou Objednateli doručeny nejpozději do 5 kalendářních dní od ukončení daného Vyhodnocovacího období. Dílčí měsíční výkazy schválené Objednatelem budou podkladem pro fakturaci Poskytovatele ve smyslu ustanovení čl. V. odst. 3 Smlouvy. Případné výhrady Objednatele k poskytnutí Průběžně poskytovaných Služeb dle předloženého Dílčího měsíčního výkazu budou řešeny vzájemnou dohodou Smluvních stran.
5. Nebyly-li Průběžně poskytované služby poskytnuty řádně, bude Dílčí měsíční výkaz vyčíslovat příslušnou smluvní pokutu v souladu s článkem XV. Smlouvy.
6. Poskytovatel neodpovídá za nedodržení SLA v případě, že takové nedodržení bylo způsobeno zásahem vyšší moci.
7. Doba, po kterou existovala překážka vyšší moci dle předchozího odstavce Smlouvy, bude zachycena v Dílčích měsíčních výkazech s jednoznačným označením.
8. Ve vztahu k Průběžně poskytovaným Službám se Poskytovatel dále zavazuje písemně oznámit Objednateli požadovaný termín a rozsah odstávky Systému a též požadované termíny výluky Průběžně poskytovaných Služeb za účelem plánované údržby Systému (dále jen „***Odstávka systému***“), alespoň 10 pracovních dnů předem. Odstávka systému je možná pouze se souhlasem Objednatele. Objednatel se zavazuje, že svůj souhlas nebude bezdůvodně odpírat. Pokud nebude souhlas udělen ve vztahu ke konkrétnímu termínu, není Poskytovatel oprávněn takovouto Odstávku systému provést a Objednatel je povinen bezodkladně navrhnout nový termín pro Odstávku systému.

VIII. POSKYTOVÁNÍ SLUŽEB NA OBJEDNÁVKU

1. Poskytovatel je povinen Objednateli poskytovat Služby na objednávku na základě objednávek Objednatele. Každá Služba na objednávku se řídí touto Smlouvou a jednotlivými ujednáními obsaženými v objednávce.
2. Sjednání Služeb na objednávku bude probíhat následovně:
   2.1. V průběhu doby trvání této Smlouvy je Objednatel oprávněn kdykoli zaslat Poskytovateli požadavek na poskytnutí Služeb na objednávku, a to formou doručení písemného požadavku datovou zprávou doručenou prostřednictvím informačního systému datových schránek, e-mailovou zprávou nebo prostřednictvím helpdesku Objednatele (dále jen „***Požadavek***“). Požadavek není návrhem na uzavření smlouvy.
   2.2. Neurčí-li Objednatel v Požadavku lhůtu delší, nebo nedohodnou-li se Smluvní strany jinak, zavazuje se Poskytovatel do deseti (10) pracovních dnů od doručení Požadavku Poskytovateli doručit datovou zprávou doručenou prostřednictvím informačního systému datových schránek, e-mailovou zprávou nebo prostřednictvím helpdesku Objednatele cenovou nabídku na realizaci Požadavku, která musí obsahovat minimálně:
      i. odkaz na tuto Smlouvu;
      ii. označení Smluvních stran;

iii. předmět Služeb na objednávku včetně jeho specifikace;
iv. termín plnění (harmonogram);
v. cenovou nabídku vycházející z cen za jednu (1) člověkohodinu strávenou na poskytování Služby na objednávku určenou na základě poctivě a v dobré víře Poskytovatelem uskutečněného posouzení pracnosti poptávané Služby na objednávku; a
vi. akceptační kritéria pro předmět příslušných Služeb na objednávku, která Poskytovatel předem projedná se zmocněncem Objednatele pro jednání věcná a technická.

(dále jen „***Nabídka***“)

Doba platnosti Nabídky je vždy minimálně třicet (30) kalendářních dnů ode dne jejího doručení Objednateli. V případě, že v Nabídce chybí některá z výše uvedených náležitostí, nemá to vliv na její závaznost pro Poskytovatele.

2.3. Na základě písemné objednávky Objednatele, která představuje odsouhlasení Nabídky, doručené Poskytovateli datovou zprávou doručenou prostřednictvím informačního systému datových schránek, e-mailovou zprávou nebo prostřednictvím helpdesku Objednatele se Poskytovatel zavazuje poskytovat Služby na objednávku uvedené v Nabídce (dále jen „***Objednávka***“). Objednávka se stává pro Smluvní strany závaznou okamžikem jejího doručení Poskytovateli.

2.4. Pro vyloučení pochybností se Smluvní strany dohodly, že doručování Nabídky a Objednávky, spolu s jejich případnými přílohami nebo dodatky, bude probíhat pouze způsoby určenými v tomto článku Smlouvy.

3. Při testování, implementaci a evidenci je Poskytovatel povinen postupovat v souladu s interní dokumentací Objednatele, se kterou byl prokazatelně seznámen.

4. Na vztahy související se Službami na objednávku se užijí ustanovení smlouvy o dílo dle § 2586 a násl. Občanského zákoníku. Výsledek poskytnutých Služeb na objednávku bude akceptován na základě akceptačního řízení.

5. Akceptační řízení zahrnuje ověření, zda plnění poskytnuté Poskytovatelem dle této Smlouvy vedlo k výsledku, ke kterému se Smluvní strany zavázaly, a to porovnáním skutečných vlastností jednotlivých výsledků plnění poskytnutých Poskytovatelem s jejich specifikací a požadavky uvedenými v Objednávce nebo stanovenými na základě této Smlouvy, přičemž specifikací se rozumí rovněž akceptační kritéria, byla-li v souladu s touto Smlouvou stanovena.

6. Objednatel vyhotoví o provedení každého akceptačního řízení protokol (dále jen „***Protokol o akceptačním řízení***“).

7. Akceptační řízení probíhá následovně:

7.1. Poskytovatel písemně informuje Objednatele o termínu předložení výsledku plnění Poskytovatele k akceptaci Objednateli nejpozději 5 pracovních dnů před předložením výsledku plnění Poskytovatele k akceptaci.

7.2. Poskytovatel předloží Objednateli k akceptaci výsledek plnění Poskytovatele, který je předmětem akceptačního řízení, a to tak, aby výsledek plnění Poskytovatele byl Objednateli řádně předán v termínu stanoveném v souladu s touto Smlouvou nebo Objednávkou. Poskytovatel je v souvislosti s rozvojem Systému povinen provést potřebnou aktualizaci dokumentace k Systému, přičemž tato aktualizace je součástí plnění dle Objednávky. Poskytovatel je povinen aktualizovanou dokumentaci předat Objednateli současně s předložením výsledku plnění dle Objednávky. Zpracována bude minimálně uživatelská a administrátorská dokumentace. Bližší podrobnosti může stanovit Objednávka.

7.3. Objednatel se zavazuje oznámit veškeré jím zjištěné vady a své výhrady nebo připomínky k výsledku plnění Poskytovatele předloženému k akceptaci do 5 pracovních dnů od jeho předložení Objednateli, nebo do 10 pracovních dnů po předložení Objednateli, pokud byla porušena povinnost Poskytovatele dle odst. 7.1. tohoto článku Smlouvy. Pokud Objednatel nesplní svou povinnost dle tohoto odstavce Smlouvy ve stanovené lhůtě, je v prodlení. Poskytovatel není v prodlení s plněním termínů dle Objednávky a této Smlouvy po dobu, ve které je Objednatel v prodlení s plněním svých povinností dle tohoto odstavce Smlouvy. Termíny dle Objednávky a této Smlouvy se o tuto dobu prodlení Objednatele prodlužují.

7.4. V případě, že výsledek plnění Poskytovatele neobsahuje dle Objednatele žádnou vadu a Objednatel nemá k výsledku plnění Poskytovatele žádné výhrady ani připomínky, je výsledkem akceptačního řízení „Akceptováno bez výhrad“. Smluvní strany považují v takovém případě výsledek plnění Poskytovatele za Poskytovatelem řádně předaný a Objednatelem řádně převzatý.

7.5. V případě, že výsledek plnění Poskytovatele obsahuje dle Objednatele drobné vady, které samostatně ani ve spojení s jinými nebrání užívání výsledku plnění Poskytovatele, nebo Objednatel má k výsledku plnění Poskytovatele nepodstatné výhrady či připomínky, je výsledkem akceptačního řízení „Akceptováno s výhradou“. V takovém případě bude Protokol o akceptačním řízení obsahovat soupis Objednatelem vytknutých vad, výhrad či připomínek a také způsoby a přiměřené lhůty pro jejich odstranění, na kterých se Smluvní strany dohodly. Smluvní strany považují v takovém případě výsledek plnění Poskytovatele za Poskytovatelem řádně předaný a Objednatelem řádně převzatý, pakliže však nebudou Objednatelem vytknuté vady, výhrady či připomínky odstraněny v souladu s Protokolem o akceptačním řízení, vzniká Objednateli nárok na smluvní pokutu dle této Smlouvy. Poskytovatel písemně informuje Objednatele o odstranění vad, výhrad či připomínek a předá Objednateli nový výsledek plnění Poskytovatele či jeho příslušnou část. Objednatel nový výsledek plnění Poskytovatele či jeho příslušnou část do 5 pracovních dnů od jeho předložení Objednateli posoudí a Poskytovateli odstranění Objednatelem vytknutých vad, výhrad či připomínek písemně potvrdí.

7.6. V případě, že výsledek plnění Poskytovatele obsahuje dle Objednatele vady jiné než drobné vady nebo Objednatel má k výsledku plnění Poskytovatele podstatné výhrady či připomínky, je výsledkem akceptačního řízení „Neakceptováno“. V takovém případě bude Protokol o akceptačním řízení obsahovat soupis Objednatelem vytknutých vad, výhrad či připomínek. Smluvní strany nepovažují v takovém případě výsledek plnění Poskytovatele za Poskytovatelem řádně předaný a Poskytovatel se může dostat do prodlení s předáním výsledku plnění Poskytovatele dle této Smlouvy. Poskytovatel je povinen bez zbytečného odkladu odstranit Objednatelem vytknuté vady, výhrady či připomínky nebo poskytnout nové plnění. Akceptační řízení dle odst. 7. tohoto článku Smlouvy se v tomto případě opakuje, dokud nebude výsledek plnění Poskytovatele Objednatelem akceptován s výsledkem „Akceptováno bez výhrad“ nebo „Akceptováno s výhradami“.

7.7. Nesdělení některé výhrady či připomínky nebo neoznámení některé vady výsledku plnění Poskytovatele v rámci akceptačního řízení nemá vliv na povinnost Poskytovatele tuto vadu odstranit, pokud o ní ví, nebo ji dodatečně zjistí či mu bude dodatečně oznámena, pakliže tato vada byla ve výsledku plnění Poskytovatele v okamžiku jeho předání Objednateli již obsažena.

8. Lhůty uvedené v předchozím odstavci platí, pokud se Smluvní strany nedohodnou písemně jinak.

9. Provedení akceptačního řízení nemá vliv na termíny stanovené v souladu s touto Smlouvou pro předání výsledku plnění Poskytovatele Objednateli.

10. Akceptací výsledku plnění Poskytovatele dle této Smlouvy v rámci akceptačního řízení s výsledkem „Akceptováno bez výhrad“ nebo „Akceptováno s výhradami“ se předmětný závazek Poskytovatele dle jednotlivé Objednávky považuje za splněný a výsledek plnění Poskytovatele je Objednateli předán k užívání.

IX. PRÁVA A POVINNOSTI SMLUVNÍCH STRAN

1. V rámci realizace předmětu plnění Smlouvy má každá Smluvní strana zejména následující povinnosti:

1.1. vzájemně spolupracovat a poskytovat druhé Smluvní straně veškeré informace potřebné pro řádné plnění svých povinností vyplývajících ze Smlouvy;

1.2. neprodleně informovat druhou Smluvní stranu o vzniku nebo hrozícím vzniku překážky plnění mající významný vliv na řádné a včasné plnění dle Smlouvy;

1.3. poskytovat druhé Smluvní straně úplné, pravdivé a včasné informace o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění dle Smlouvy;

1.4. plnit své povinnosti vyplývající ze Smlouvy tak, aby nedocházelo k prodlení s plněním povinností vázaných k jednotlivým termínům a úhradě splatných jednotlivých peněžních dluhů.

2. V rámci poskytování Služeb má Poskytovatel zejména následující povinnosti:

   2.1. postupovat při plnění Smlouvy řádně tak, aby bylo dosaženo účelu Smlouvy;

   2.2. poskytovat Služby v souladu se Smlouvou, řádně a včas a v souladu příslušnými obecnými standardy v odvětví a relevantními technickými normami;

   2.3. zajistit dostatečnou kapacitu svých pracovníků s odpovídající kvalifikací a zkušenostmi pro poskytování Služeb a to nejméně v rozsahu 2 dedikovaní programátoři a 3 senior konzultanti;

   2.4. poskytovat Služby v souladu s platnými a účinnými obecně závaznými právními předpisy, dle současného stavu techniky, jakož i v souladu se všemi normami obsahujícími technické specifikace a technická řešení, technické a technologické postupy nebo jiná určující kritéria, tak jak vyplývají i z relevantních právních předpisů;

   2.5. řídit se provozní, bezpečnostní a ostatní dokumentací a pravidly, týkajícími se provozu Systému;

   2.6. postupovat v profesionální kvalitě a s odbornou péčí, podle nejlepších odborných znalostí a schopností a sledovat a chránit oprávněné zájmy Objednatele.

3. Poskytovatel bere na vědomí, že plnění dle Smlouvy bude poskytovat v rámci informačních systémů základní služby, jejichž správcem je Objednatel. S ohledem na uvedené je Poskytovatel povinen poskytovat plnění dle Smlouvy zejm. v souladu se zákonem o kybernetické bezpečnosti a v souladu s vyhláškou o kybernetické bezpečnosti, resp. tak, aby se Poskytovatel vyvaroval jakékoliv činnosti, jež by mohla být označena za porušení uvedených právních předpisů Objednatelem.

4. Poskytovatel je povinen zachovat bezpečnost informací a dat obsažených v informačních systémech základní služby spravovaných Objednatelem, včetně jiných informačních systémů, které budou plněním Smlouvy dotčeny, a to zejm. z pohledu důvěrnosti, dostupnosti a integrity. Plnění dle Smlouvy je Poskytovatel povinen poskytovat tak, aby důvěrnost, dostupnost a integrita informací a dat dle předchozí věty nebyla přerušena, ohrožena, ani omezena. Je-li k plnění dle Smlouvy nezbytné důvěrnost, dostupnost či integritu dat omezit, ohrozit nebo přerušit, může tak Poskytovatel učinit pouze po předchozím souhlasu Objednatele a jen v rozsahu Objednatelem předem odsouhlaseném.

5. Poskytovatel není oprávněn užít informace ani data obsažená v informačních systémech základní služby spravovaných Objednatelem, ani v jiných informačních systémech, které budou plněním Smlouvy dotčeny. Je-li užití informací či dat dle předchozí věty nezbytné k plnění dle Smlouvy, může je Objednatel využít jen po předchozím souhlasu Objednatele a jen v rozsahu Objednatelem předem odsouhlaseném.

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

7. Poskytovatel se zavazuje, že na Pracovišti neponechá volně dostupná instalační, záložní nebo archivní média ani dokumentaci k Systému nebo k jeho HW komponentám, které jsou předmětem plnění dle Smlouvy. HW komponentou se rozumí každý HW prvek, který je nosičem dat, ukládá nebo třídí data Systému a/nebo je ovládán SW, který je součástí Systému.

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

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

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

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

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

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

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

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

16. Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli v Systému:
    a) neukládaly a/nebo nesdílely data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele,
    b) nestahovaly, nesdílely, neukládaly, nearchivovaly a/nebo neinstalovaly datové a spustitelné soubory v rozporu s licenčními podmínkami nebo zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „autorský zákon“),
    c) nezasílaly řetězové emaily.

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

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

19. Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli, které přistupují do interní sítě a/nebo Systému Objednatele chránily autentizační prostředky a údaje k Systému Objednatele.

20. Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako kybernetická bezpečnostní událost ve smyslu příslušné řídící dokumentace a mohou být uplatněny příslušné postupy zvládání kybernetické bezpečnostní události (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu). Poskytovatel bere na vědomí, že postup zvládáním kybernetické bezpečnostní události či jiný důsledek porušení Bezpečnostních opatření nebude posuzován jako okolnost vylučující odpovědnost Poskytovatele za prodlení s řádným a včasným plněním předmětu Smlouvy a nebude důvodem k jakékoli náhradě případné újmy Poskytovateli či jiné osobě ze strany Objednatele.

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

22. Objednatel je oprávněn přiměřeně a v nezbytném rozsahu kdykoliv a jakýmkoliv způsobem zkontrolovat, zda Poskytovatel řádně splnil či plní veškeré povinnosti, které Poskytovateli ze Smlouvy vyplývají. Objednatel je oprávněn kontrolu či audit provádět i v provozovnách Poskytovatele a na jiných místech, kde Poskytovatel provádí činnosti, které souvisí s činností Poskytovatele dle Smlouvy. Poskytovatel je povinen poskytnout Objednateli ke kontrole či auditu veškerou potřebnou součinnost.

23. Objednatel bude provádět audit rizik ve smyslu § 8 vyhlášky o kybernetické bezpečnosti, jehož cílem je ověřovat vývoj přijatých opatření a požadavků Objednatele. Objednatel bude v rámci provádění auditu rizik preferovat důkazní doložení skutečností (např. e-mailem) před místním šetřením. Bližší podmínky řízení dodavatelů jsou uvedeny v Metodice řízení dodavatelů (Příloha č. 5 Smlouvy) a v Nástroji pro hodnocení dodavatele dle VKB (Příloha č. 6 Smlouvy)

(dále jen „***Nástroj pro hodnocení dodavatele dle VKB***“). Audit rizik bude prováděn vždy minimálně jednou ročně. Poskytovatel je povinen podrobit se, strpět a poskytovat Objednateli součinnost v rámci provádění auditu rizik.

24. Objednatel provedl úvodní audit rizik již v rámci Řízení veřejné zakázky (dále jen „***Úvodní audit rizik***“), přičemž výchozí celková hodnota hodnocení Poskytovatele činí 31,82 % (dále jen „***Výchozí hodnota***“).

25. Poskytovatel je povinen přijímat taková opatření, aby jeho celková hodnota hodnocení dle Nástroje pro hodnocení dodavatele dle VKB v průběhu plnění Smlouvy rostla, přičemž takový růst musí činit vždy nejméně 10 % oproti Výchozí hodnotě, jedná-li se o první audit rizik prováděný dle Smlouvy po Úvodním auditu rizik, nebo oproti předchozí hodnotě, jedná-li se o všechny další audity rizik prováděné dle Smlouvy. Povinnost dle předchozí věty tohoto odstavce Smlouvy se vztahuje ke každému provedenému auditu rizik, pokud od účinnosti Smlouvy (okamžik stanovení Výchozí hodnoty), nebo od okamžiku stanovení předchozí hodnoty, uplynulo nejméně 10 měsíců.

26. Jestliže Poskytovatel dosáhne celkové hodnoty hodnocení 80 %, není již povinen přijímat opatření za účelem růstu celkové hodnoty hodnocení ve smyslu předchozího odstavce Smlouvy, nicméně je nadále povinen podrobit se, strpět a poskytovat Objednateli součinnost v rámci provádění auditu rizik. Jestliže Poskytovatel opět poklesne na celkovou hodnotu hodnocení nižší než 80 % je opět povinen postupovat podle předchozího odstavce Smlouvy.

27. Poskytovatel je povinen dodržovat při plnění Smlouvy veškerou aktuální bezpečnostní politiku a předpisy Objednatele, které mu byly Objednatelem předány nebo se kterými byl Objednatelem seznámen a které mají dopad na plnění Poskytovatele dle této Smlouvy. Bezpečnostní politikou a předpisy Objednatele, které mají dopad na plnění Poskytovatele dle této Smlouvy, se rozumí bezpečnostní dokumentace, která se vztahuje k plnění Poskytovatele dle této Smlouvy nebo se obvykle vztahuje k povinnostem subjektů, které jsou v dodavatelském vztahu k Objednateli, s přihlédnutím ke skutečnosti, že Objednatel je správcem a provozovatelem informačního systému základní služby. Objednatel je povinen Poskytovateli předat nebo Poskytovatele seznámit s aktuální bezpečnostní politikou a předpisy Objednatele, které mají dopad na plnění Poskytovatele dle této Smlouvy, o čemž bude vždy vyhotoven zápis podepsaný oběma Smluvními stranami.

28. Poskytovatel je povinen v průběhu plnění této Smlouvy průběžně spolupracovat s garantem aktiva Objednatele za účelem identifikace významných změn a jejich dopadů do oblasti kybernetické bezpečnosti Objednatele v souladu s § 11 vyhlášky o kybernetické bezpečnosti souvisejících s předmětem plnění dle této Smlouvy. Metodika hodnocení rizik je uvedena v Příloze č. 8 této Smlouvy. V případě identifikace významných změn souvisejících s předmětem plnění dle této Smlouvy se Poskytovatel zavazuje spolupracovat s Objednatelem na identifikaci potencionálních rizik možných dopadů významných změn a v případě potřeby poskytne Objednateli informace o možných opatřeních pro snížení nepříznivých možných dopadů spojených s významnými změnami, o možnosti zajištění jejich testování a možnosti navrácení významných změn do původního stavu v případě jejich realizace, a to na základě informací, které jsou Poskytovateli známé nebo mu být známé měly.

29. Poskytovatel je povinen poskytnout plnění dle Smlouvy řádně v souladu se Smlouvou a veškerými jejími přílohami a českými i evropskými právními předpisy platnými a účinnými v době poskytování plnění.

30. V případě výskytu kybernetického bezpečnostního incidentu souvisejícího s předmětem plnění dle této Smlouvy u Poskytovatele, je Poskytovatel povinen o něm Objednatele neprodleně písemně informovat, a to nejpozději do následujícího dne po zjištění kybernetického bezpečnostního incidentu. Součástí informace o kybernetickém bezpečnostním incidentu jsou:

    30.1. identifikace části Systému, kde ke kybernetickému bezpečnostnímu incidentu došlo nebo na kterou má kybernetický bezpečnostní incident dopad;

    30.2. datum a čas zjištění kybernetického bezpečnostního incidentu;

    30.3. popis kybernetického bezpečnostního incidentu.

    Poskytovatel a Objednatel se zavazují vzájemně spolupracovat na řešení dopadu kybernetického bezpečnostního incidentu a na nápravných opatřeních směřujících k minimalizaci rizik, která měla vliv na vznik kybernetického bezpečnostního incidentu.

31. Poskytovatel je povinen informovat Objednatele o způsobu řízení rizik na straně Poskytovatele a o zbytkových rizicích souvisejících s plněním této Smlouvy, a to neprodleně od nabytí účinnosti této Smlouvy a poté vždy neprodleně od každé změny předtím Poskytovatelem

Objednateli poskytnutých informací o způsobu řízení rizik na straně Poskytovatele a o zbytkových rizicích souvisejících s plněním této Smlouvy. Poskytovatel je povinen informovat Objednatele o zbytkových rizicích ve formátu „riziko – bezpečností opatření – zbytkové riziko“.

32. Poskytovatel se zavazuje, že jakoukoliv změnu v osobě ovládající Poskytovatele ve smyslu § 71 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších přepisů (dále jen „***ZOK***“) bez zbytečného odkladu po uskutečnění takové změny písemně oznámí Objednateli.

33. Poskytovatel se zavazuje, že jakoukoliv změnu vlastnictví zásadních aktiv, popřípadě změnu oprávnění nakládat s těmito aktivy, využívaných Poskytovatelem k plnění podle této Smlouvy, bez zbytečného odkladu po uskutečnění takové změny písemně oznámí Objednateli.

34. Poskytovatel se zavazuje poskytnout Objednateli součinnost při výběru dodavatele na poskytování služeb týkajících se Systému, a to poskytnutím nebo zpřístupněním informací, dat, provozních údajů či dokumentací týkajících se předmětu plnění této Smlouvy, které jsou nezbytné k provedení výběru takového dodavatele.

35. Dojde-li k ukončení této Smlouvy, je Poskytovatel povinen dle pokynů Objednatele učinit veškerá nezbytná bezpečnostní opatření ve smyslu zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti tak, aby takovým ukončením Smlouvy nedošlo k narušení bezpečnosti informačních systémů základní služby, jejichž je Objednatel správcem. Poskytovatel je povinen zajistit veškerou potřebnou součinnost Objednateli při jakémkoli ukončení této Smlouvy tak, aby fungování Systému bylo plně zajištěno jinou odborně způsobilou osobou. Do doby zajištění fungování Systému jinou odborně způsobilou osobou je Poskytovatel povinen vyvinout maximální možnou součinnost se zajištěním řádného fungování Systému, a to i nad rámec závazků vyplývajících z této Smlouvy (např. poskytnutí součinnosti v přechodném období při ukončení spolupráce, kdy je třeba ještě udržovat službu před nasazením nového řešení, migrace dat a podobně), bude-li to pro bezvadné fungování Systému nezbytné.

36. Poskytovatel se zavazuje poskytnout Objednateli součinnost při řízení kontinuity činností týkající se předmětu plnění této Smlouvy.

37. Bude-li Poskytovatel na základě této Smlouvy Objednateli předávat v elektronické podobě jakékoliv informace, data, provozní údaje nebo dokumentaci či informace po vyžádání správcem Objednatele, je povinen je Objednateli předat tak, aby byly pro Objednatele dále použitelné, a to obvykle v systematizované podobě a v otevřeném a strojově čitelném formátu, např. *.pdf nebo *.doc či *.docx.

38. Získá-li Poskytovatel v souvislosti s plněním této Smlouvy jakákoliv data, která nebudou nezbytná pro splnění předmětu této Smlouvy, neprodleně taková data zlikviduje v souladu s pokyny Objednatele a pravidly vyplývajícími z vyhlášky o kybernetické bezpečnosti. Likvidaci ostatních získaných dat Poskytovatel provede stejným způsobem, a to neprodleně po splnění předmětu této Smlouvy. Poskytovatel je povinen si vždy před provedením likvidace dat vyžádat pokyny Objednatele.

39. Objednatel se zavazuje poskytnout ke splnění smluvních závazků Poskytovatele účelnou součinnost, dokumentaci a informace definované v této Smlouvě nebo potřebné pro účelné plnění předmětu této Smlouvy, a dále bude Poskytovatele včas informovat o všech organizačních změnách, poznatcích z kontrolní činnosti, podnětech vlastních zaměstnanců a dalších skutečnostech významných pro plnění předmětu této Smlouvy.

40. Poskytovatel se zavazuje zachovat kontinuitu stávající podpory, která je součástí předchozího plnění stávajícího poskytovatele servisní služby (maintenance, podpora provozu, servis, rozvoj Systému a poskytování dalších služeb), která je definována výpisem z HelpDesku stávajícího poskytovatele s určenou prioritou a předpokládaným termínem plnění, jak je uvedeno v rámci Přílohy č. 7 Smlouvy - Zachování kontinuity podpory.

X. VLASTNICKÉ PRÁVO A UŽÍVACÍ PRÁVA

1. V případě, že součástí plnění Poskytovatele dle této Smlouvy jsou movité věci, které se mají stát vlastnictvím Objednatele, nabývá Objednatel vlastnické právo k těmto věcem dnem podpisu příslušného Protokolu o akceptačním řízení. Ke stejnému dni přechází na Objednatele také nebezpečí škody na předaných věcech. Do nabytí vlastnického práva uděluje Poskytovatel. Objednateli právo tyto věci užívat v rozsahu a způsobem, který vyplývá z účelu této Smlouvy.

2. Bude-li výsledkem plnění Poskytovatele dle této Smlouvy předmět naplňující znaky autorského díla (dále jen „***Autorské dílo***“ či „***Autorská díla***“) ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „***Autorský zákon***“), nabývá Objednatel dnem poskytnutí Autorského díla Objednateli k užívání dle této Smlouvy právo užívat takové Autorské dílo (dále jen „***Licence***“).

3. Licence se poskytuje, resp. musí být poskytnuta:

   3.1. jako úplatná, přičemž úplata je zahrnuta v Ceně Služeb dle čl. IV. odst. 1 Smlouvy;

   3.2. jako neomezená nevýhradní;

   3.3. z hlediska časového rozsahu minimálně na dobu trvání všech majetkových práv k předmětu Licence;

   3.4. z hlediska územního rozsahu jako neomezená;

   3.5. z hlediska věcného rozsahu (způsobu užití) tak, že opravňuje ke všem známým a možným způsobům užití, které povaha Služeb připouští, a které nejsou v rozporu s právními předpisy, zejména k takovým způsobům užití, jež jsou potřebná nebo nezbytná k tomu, aby bylo možné užívat Služby k účelu sjednanému Smlouvou nebo účelu ze Smlouvy vyplývajícímu;

   3.6. z hlediska osobního rozsahu (multilicence), resp. množství jako neomezená.

4. Objednatel není povinen Licenci využít.

5. Poskytovatel tímto jménem všech autorů Autorských děl:

   5.1. bezplatně uděluje Objednateli oprávnění Autorská díla zveřejnit a jakýmkoliv způsobem měnit, tedy zejm. je jakkoliv upravovat, dělit, rozšiřovat, spojovat s díly jinými, zařadit do díla souborného apod.;

   5.2. zmocňuje Objednatele, aby jménem všech autorů Autorských děl uděloval třetím osobám oprávnění Autorská díla zveřejnit a jakýmkoliv způsobem měnit, tedy zejm. je jakkoliv upravovat, dělit, rozšiřovat, spojovat s díly jinými, zařadit do díla souborného apod.;

   5.3. uděluje Objednateli oprávnění zmocnit jménem všech autorů Autorských děl třetí osoby k udělení oprávnění jiným třetím osobám ke zveřejnění nebo jakékoliv změně Autorských děl v rozsahu dle čl. X. odst. 5.1. Smlouvy jménem všech autorů Autorských děl.

6. Součástí Licence je rovněž neomezené právo Objednatele poskytnout třetím osobám podlicenci k užití Autorského díla v rozsahu shodném s rozsahem Licence a souhlas Poskytovatele k postoupení Licence na třetí osoby a nepožaduje sdělení, zda a komu byla Licence (podlicence) poskytnuta nebo postoupena.

7. Licence se automaticky vztahuje i na všechny nové verze, aktualizované verze, i na úpravy a překlady Autorského díla poskytnuté Poskytovatelem.

8. Poskytuje-li Poskytovatel Licenci k počítačovým programům vyvíjeným Poskytovatelem (popř. jeho poddodavatelem nebo jinou třetí osobou), vztahuje se Licence ve stejném rozsahu k počítačovým programům ve zdrojovém a strojovém kódu, jakož i ke koncepčním přípravným materiálům, a to i na případné další verze počítačových programů. Zdrojové kódy budou Objednateli poskytnuty za podmínek stanovených v článku XI. Smlouvy.

9. Do té doby, než bude Autorské dílo poskytnuto Objednateli k užívání dle odst. 2. tohoto článku Smlouvy je Objednatel oprávněn Autorské dílo užívat v rozsahu a způsobem nezbytným k provedení akceptace výsledku plnění Poskytovatele dle této Smlouvy.

10. Smluvní strany výslovně prohlašují, že pokud při poskytování plnění dle této Smlouvy vznikne činností Poskytovatele a Objednatele dílo spoluautorů a nedohodnou-li se Smluvní strany výslovně jinak, bude se mít za to, že je Objednatel oprávněn vykonávat majetková autorská práva k dílu spoluautorů tak, jako by byl jejich výlučným vykonavatelem a že Poskytovatel udělil Objednateli souhlas k jakékoliv změně nebo jinému zásahu do díla spoluautorů. Cena Služby je stanovena se zohledněním tohoto ustanovení a Poskytovateli nevzniknou v případě vytvoření díla spoluautorů žádné nové nároky na odměnu.

11. Bude-li Autorské dílo vytvořeno činností Poskytovatele, Smluvní strany činí nesporným, že jakékoliv takové Autorské dílo vzniklo z podnětu a pod vedením Objednatele.

12. Součástí výsledku plnění Poskytovatele dle této Smlouvy může být tzv. proprietární (standardní) software (dále jen „***Proprietární software***“), u kterého Poskytovatel nemůže Objednateli

poskytnout oprávnění dle předchozích ustanovení tohoto článku X Smlouvy nebo to po něm nelze spravedlivě požadovat, to však pouze při splnění některé z následujících podmínek:

12.1. jedná se o software renomovaných výrobců, jenž je na trhu běžně dostupný, tj. nabízený na území České republiky alespoň třemi na sobě nezávislými a vzájemně nepropojenými subjekty oprávněnými takovýto software upravovat, a který je v době uzavření smlouvy prokazatelně užíván v produktivním prostředí nejméně u deseti na sobě nezávislých a vzájemně nepropojených subjektů. Poskytovatel je povinen poskytnout Objednateli o této skutečnosti písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat.

12.2. jedná se o tzv. open source software, který je veřejnosti poskytován zdarma, včetně zdrojových kódů, úplné uživatelské, provozní a administrátorské dokumentace a práva software měnit. Poskytovatel je povinen poskytnout Objednateli o této skutečnosti písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat.

12.3. jedná se o software, u kterého Poskytovatel poskytne s ohledem na jeho (i) marginální význam, (ii) nekomplikovanou propojitelnost či (iii) oddělitelnost a nahraditelnost v rámci výsledku plnění Poskytovatele dle této Smlouvy bez nutnosti vynakládání výraznějších prostředků, písemnou garanci, že další rozvoj výsledku plnění Poskytovatele dle této Smlouvy jinou osobou než Poskytovatelem je možné provádět bez toho, aby tím byla dotčena práva autorů takového softwaru, neboť nebude nutné zasahovat do zdrojových kódů takového softwaru anebo proto, že případné nahrazení takového softwaru nebude představovat výraznější komplikaci a náklad na straně Objednatele.

12.4. jedná se o software, k němuž Poskytovatel Objednateli poskytne nebo zprostředkuje poskytnutí úplných zdrojových kódů a bezpodmínečného práva provádět jakékoliv modifikace, úpravy, změny takového software a dle svého uvážení do něj zasahovat, zapracovávat ho do dalších autorských děl, zařazovat ho do děl souborných či do databází apod., a to i prostřednictvím třetích osob, přičemž poskytování zdrojových kódů se řídí článkem XI Smlouvy.

13. V případě Proprietárního softwaru je dostatečné, aby Poskytovatel Objednateli poskytl neomezené nevýhradní právo užívat takový Proprietární software jakýmkoli způsobem nejméně po dobu poskytování Služeb dle této Smlouvy a jeden rok po skončení trvání této Smlouvy a v množstevním rozsahu, který je nezbytný pro pokrytí potřeb Objednatele ke dni předání předmětného výsledku plnění Poskytovatele dle této Smlouvy Objednateli, a to včetně práva Objednatele do Proprietárního software zasahovat, pokud tak stanoví příslušné ustanovení odst. 12. tohoto článku Smlouvy. V případě výpovědi či odstoupení od této Smlouvy se Poskytovatel zavazuje nabídnout Objednateli právo užívat Proprietární software v rozsahu, v jakém je to nezbytné pro řádné užívání výsledků plnění Poskytovatele dle této Smlouvy. Tím není dotčeno právo Objednatele pořídit Proprietární software i od třetí osoby bez ohledu na licence pořízené dříve Poskytovatelem. V případě využití tohoto přednostního práva se Poskytovatel zavazuje, že právo užívat Proprietární software dle tohoto odstavce této Smlouvy nabídne Objednateli za běžných tržních podmínek a bude vycházet z účetní hodnoty licencí, které pořídil.

14. Nelze-li to na Poskytovateli spravedlivě požadovat, nemusí být Objednateli k Proprietárnímu softwaru předány zdrojové kódy a stejně tak nemusí být poskytnuto právo Objednatele do Proprietárního softwaru zasahovat, vždy však musí být předána kompletní uživatelská, administrátorská a provozní dokumentace.

15. Poskytovatel je povinen v rámci poskytování Služeb dle této Smlouvy omezit využití Proprietárního software.

16. Poskytovatel se zavazuje samostatně zdokumentovat veškeré využití Proprietárního software v rámci jím poskytnutých výsledků plnění dle této Smlouvy a předložit Objednateli ucelený přehled využitého Proprietárního software, jeho licenčních podmínek a jeho alternativních dodavatelů. Tento přehled je Poskytovatel povinen předložit Objednateli vždy do 3 (tří) pracovních dnů po akceptaci výsledku plnění, v jehož rámci Poskytovatel využil Proprietární software a dále vždy do 1 (jednoho) měsíce od doručení výzvy Objednatele, kterou může Objednatel učinit kdykoli, nejpozději však do 3 (tří) kalendářních let po roku, ve kterém skončilo trvání této Smlouvy.

17. Jestliže jsou s užitím Proprietárního software či jiných souvisejících plnění spojeny jednorázové či pravidelné poplatky, je Poskytovatel povinen v rámci Ceny Služeb řádně uhradit všechny tyto poplatky za celou dobu trvání licence.

18. Udělení Licence nelze ze strany Poskytovatele vypovědět a jejich účinnost trvá i po skončení účinnosti této Smlouvy, nedohodnou-li se Smluvní strany výslovně jinak.

19. Odměna za zprostředkování nebo postoupení Licence k Autorskému dílu je zahrnuta v ceně za služby, při jejichž poskytnutí došlo k vytvoření Autorského díla.

20. Práva získaná v rámci plnění této Smlouvy přecházejí i na případného právního nástupce Objednatele. Případná změna v osobě Poskytovatele (např. právní nástupnictví) nebude mít vliv na oprávnění udělená v rámci této Smlouvy Poskytovatelem Objednateli.

21. Poskytovatel je povinen postupovat tak, aby udělení Licence k Autorskému dílu dle této Smlouvy včetně oprávnění udělit podlicenci a souvisejících oprávnění zabezpečil, a to bez újmy na právech třetích osob.

22. Poskytovatel prohlašuje, že je oprávněn vykonávat svým jménem a na svůj účet majetková práva autorů k Autorským dílům, která jsou výsledkem plnění Poskytovatele dle této Smlouvy, resp. že má souhlas všech relevantních třetích osob k poskytnutí Licence k Autorským dílům podle tohoto článku X. Smlouvy; toto prohlášení zahrnuje i taková práva, která by vytvořením Autorského díla teprve vznikla.

23. Poskytovatel prohlašuje, že je oprávněn zmocnění a oprávnění dle odst. 5. tohoto článku Smlouvy a Licenci ve shora uvedeném rozsahu Objednateli poskytnout a udělit. Objednatel oprávnění a zmocnění dle odst. 5. tohoto článku Smlouvy přijímá. Poskytovatel jménem všech autorů Autorských děl s Objednatelem sjednává, že autoři Autorských děl jsou oprávněni odvolat zmocnění dle odst. 5. tohoto článku Smlouvy jen v případě, že by Objednatel při výkonu zástupčího oprávnění postupoval v rozporu s dobrými mravy.

24. Poskytovatel prohlašuje, že veškeré jím poskytnuté plnění dle této Smlouvy je prosté právních vad a zavazuje se odškodnit v plné výši Objednatele v případě, že třetí osoba úspěšně uplatní autorskoprávní nebo jiný nárok plynoucí z právní vady poskytnutého plnění. V případě, že by nárok třetí osoby vzniklý v souvislosti s poskytnutým plněním Poskytovatele dle této Smlouvy, bez ohledu na jeho oprávněnost, vedl k dočasnému či trvalému soudnímu zákazu či omezení užívání poskytnutého plnění dle této Smlouvy, zavazuje se Poskytovatel zajistit náhradní řešení a minimalizovat dopady takovéto situace, a to bez dopadu na cenu plnění sjednanou dle této Smlouvy, přičemž současně nebudou dotčeny ani nároky Objednatele na náhradu škody.

25. Poskytovatelem udělená Licence se vztahuje ve shora uvedeném rozsahu i na jakákoli rozšíření, upgrady, updaty a patche Autorských děl.

XI. ZDROJOVÝ KÓD

1. Poskytovatel je povinen současně s předáním výsledků Služeb na objednávku, které jsou počítačovým programem, předat Objednateli zdrojový kód (dále jen „***Zdrojový kód***“). Zdrojový kód dle této Smlouvy bude strukturovaný, dokumentovaný, přičemž bude možné jej přeložit a sestavit do spustitelných programů. Zdrojový kód musí být spustitelný v prostředí Objednatele a zaručovat možnost ověření, že je kompletní a ve správné verzi, tzn. umožňující kompilaci, instalaci, spuštění a ověření funkcionality, a to včetně podrobné dokumentace Zdrojového kódu takovéto části plnění dle této Smlouvy. Zdrojový kód bude Objednateli Poskytovatelem předán do sdíleného elektronického uložiště, které pro tento účel zřídí Poskytovatel a do kterého poskytne Poskytovatel Objednateli v potřebném rozsahu přístup. O předání Zdrojového kódu bude oběma Smluvními stranami sepsán a podepsán písemný předávací protokol.

2. Povinnost Poskytovatele uvedená v odst. 1 tohoto článku Smlouvy se přiměřeně použije i pro:

   2.1. jakékoliv modifikace, úpravy, opravy, změny, doplnění, upgrade nebo update Zdrojového kódu počítačového programu tvořícího výsledek Služeb na objednávku;

   2.2. jakékoliv modifikace, úpravy, opravy, změny, doplnění, upgrade nebo update Zdrojového kódu Systému, k nimž dojde při plnění této Smlouvy.

3. Dokumentace změny Zdrojového kódu musí obsahovat podrobný popis a komentář každého zásahu do Zdrojového kódu. Pro evidenci změn Zdrojového kódu je možné využití specializovaných nástrojů pro verzování změn. Poskytovatel bude odpovídat za aktuální stav obsahu Zdrojového kódu.

4. Poskytovatel je povinen předat Objednateli dokumentovanou změnu Zdrojového kódu nejpozději do 7 kalendářních dnů následujících po dni, ve kterém byla změna Zdrojového kódu uskutečněna. V případě jakéhokoli ukončení této Smlouvy z důvodu porušení Smlouvy Poskytovatelem je Poskytovatel povinen předat Objednateli aktuální Zdrojové kódy a koncepční přípravné materiály všech součástí Systému tak, aby byl Objednatel držitelem Zdrojového kódu minimálně k v dané chvíli aktuální verzi Systému.

5. Poskytovatel bere na vědomí, že Objednatel může Zdrojový kód dle odst. 1 tohoto článku Smlouvy či jeho změny dle odst. 2 tohoto článku Smlouvy neomezeně sdílet s jakoukoli třetí osobou a že jej může uveřejnit.

6. Poskytovatel bere na vědomí, že Objednatel může Zdrojový kód dle odst. 1 tohoto článku Smlouvy či jeho změny dle odst. 2 tohoto článku Smlouvy užít či zpřístupnit pro provádění modifikací, úprav, změn a rozvoje autorského díla dle článku X. této Smlouvy třetím osobám.

XII. PRÁVA K DATABÁZÍM

1. **Databáze Objednatele**

   1.1. Smluvní strany prohlašují, že práva k veškerým databázím Objednatele existujícím před uzavřením této Smlouvy nebo vytvořeným Objednatelem kdykoliv v průběhu plnění této Smlouvy, které mají být využity Poskytovatelem pro účely plnění této Smlouvy, náleží Objednateli, který je pořizovatelem databáze ve smyslu § 89 Autorského zákona.

   1.2. Objednatel v souvislosti s plněním dle této Smlouvy nepřevádí práva pořizovatele databáze ve smyslu § 90 odst. 6 Autorského zákona.

2. **Databáze vytvořené pro potřeby této Smlouvy**

   2.1. Smluvní strany prohlašují, že práva k veškerým databázím vytvořeným Poskytovatelem pro účely plnění této Smlouvy náleží Objednateli, který je pořizovatelem databáze ve smyslu § 89 Autorského zákona.

   2.2. Objednatel v souvislosti s plněním dle této Smlouvy nepřevádí práva pořizovatele databáze ve smyslu § 90 odst. 6 Autorského zákona.

3. Smluvní strany potvrzují, že s ohledem na práva Objednatele k databázím specifikovaným v odst. 1. a 2. tohoto článku Smlouvy je Poskytovatel oprávněn užívat databáze pouze v rozsahu a způsobem nezbytným pro provoz, správu a rozvoj předmětu plnění dle Smlouvy.

4. Součástí práva k databázím dle odst. 1. a 2. tohoto článku Smlouvy je též právo Objednatele vytěžovat a zužitkovávat celý obsah databází za účelem jeho zpracování pro výsledné zobrazení výsledku zpracování.

5. Poskytovatel se zavazuje poskytnout Objednateli veškerou potřebnou součinnost, pro likvidaci nepotřebných dat, za tím účelem smluvní strany dohodnou lhůty pro provádění likvidace dat, kde určí konkrétní rozsah a časové intervaly pro likvidaci dat. Smluvní strany sjednávají, že k likvidaci dat přistoupí po vzájemném odsouhlasení likvidace, podmínky likvidace musí být v souladu Přílohou č. 4 Vyhlášky o kybernetické bezpečnosti.

XIII. POJIŠTĚNÍ

1. Poskytovatel se zavazuje, že bude mít po celou dobu trvání závazků Poskytovatele vyplývajících ze Smlouvy sjednáno pojištění odpovědnosti za škodu či jinou újmu způsobenou Poskytovatelem při výkonu činnosti jiné osobě s limitem pojistného plnění minimálně ve výši 5 000 000,- Kč. V případě, že Smlouvu uzavřelo na straně Poskytovatele více osob (členů sdružení, členů společnosti apod.), musí pojistná smlouva prokazatelně pokrývat případnou škodu či jinou újmu způsobenou kteroukoli z těchto osob.

2. Poskytovatel je povinen předložit Objednateli pojistnou smlouvu nebo certifikát o pojištění osvědčující splnění povinnosti Poskytovatele podle předchozího odstavce této Smlouvy kdykoli v průběhu trvání závazků z této Smlouvy, a to do 3 pracovních dnů ode dne, kdy k tomu byl Objednatelem písemně vyzván.

3. Poskytovatel i Objednatel se zavazují uplatnit pojistnou událost u pojišťovny bez zbytečného odkladu.

XIV. MLČENLIVOST A OCHRANA OSOBNÍCH ÚDAJŮ

1. Vzhledem k tomu, že na základě plnění této Smlouvy bude docházet ke zpracování osobních údajů Poskytovatelem pro Objednatele, dohodly se Smluvní strany ve smyslu čl. 28 odst. 3 Nařízení 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 (dále jen „**GDPR**“) na podmínkách zpracování těchto osobních údajů, které jsou stanoveny níže v tomto článku této Smlouvy.

2. Smluvní strany se dohodly, že pokud to bude potřebné ke splnění požadavků předpisů na ochranu osobních údajů (zejména zákon č. 110/2019 Sb. o zpracování osobních údajů, ve znění pozdějších předpisů, a GDPR; dále jen „**POOÚ**“), uzavřou bez zbytečného odkladu po výzvě kterékoli Smluvní strany písemný dodatek této Smlouvy zohledňující takové požadavky. Uzavřením takového dodatku nevzniká Poskytovateli jakýkoli nárok na navýšení ceny poskytovaných Služeb.

3. Objednatel tímto pověřuje Poskytovatele zpracováním osobních údajů subjektů údajů poskytovaných Objednatelem v souvislosti s plněním dle této Smlouvy. Poskytovatel je povinen zpracovávat osobní údaje pro Objednatele na základě jeho pokynů a v rozsahu nezbytném k řádnému plnění povinností Poskytovatele vyplývajících z této Smlouvy

4. Předmětem zpracování jsou osobní údaje subjektů údajů, kterými jsou pacienti, jimž jsou Objednatelem poskytovány zdravotní služby, a dále zaměstnanci Objednatele, kteří jsou poskytovateli zdravotních služeb a případně další osoby evidované v Systému Objednatele (dále jen „**Subjekty údajů**“).

5. Předmětem zpracování jsou osobní údaje nebo zvláštní kategorie osobních údajů (citlivé údaje) Subjektů údajů obsažené v Systému, a to zejména adresní a identifikační údaje Subjektů údajů, a dále i citlivé osobní údaje pacientů uvedené ve zdravotnické dokumentaci a/ nebo osobní údaje dalších osob evidovaných v tomto Systému, jejichž osobní údaje poskytl Objednatel či třetí strany z pokynu Objednatele Poskytovateli (dále společně jen „**Osobní údaje**“).

6. Účel zpracování Osobních údajů je definován účelem plnění této Smlouvy, případně dalšími účely, které vyplývají z této Smlouvy a jejích příloh.

7. Zpracování Osobních údajů bude probíhat po dobu účinnosti této Smlouvy. Povinnosti Poskytovatele týkající se ochrany osobních údajů se Poskytovatel zavazuje plnit po celou dobu účinnosti této Smlouvy, pokud z této Smlouvy nevyplývá, že mají trvat i po zániku její účinnosti. Poskytovatel je zejména při zpracování Osobních údajů povinen:

   7.1. zpracovávat Osobní údaje výlučně na základě doložených pokynů Objednatele, za účelem a v nezbytně nutném rozsahu stanoveném v této Smlouvě a v přímé souvislosti s poskytováním plnění dle této Smlouvy; pro vyloučení pochybností zpracování Osobních údajů v souladu s povinnostmi Poskytovatele dohodnutými v rámci této Smlouvy se považuje za prováděné v souladu s instrukcemi Objednatele, nedohodnou-li se Smluvní strany v konkrétním případě písemně jinak nebo neudělí-li Objednatel v konkrétním případě jiné specifické instrukce;

   7.2. řídit se instrukcemi Objednatele v otázkách předání Osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládá právo Evropské unie nebo členského státu, které se na objednatele vztahuje; v takovém případě PoskytovatelObjednatele informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu;

   7.3. zajišťovat, aby se osoby oprávněné zpracovávat Osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;

   7.4. vést záznamy o činnostech zpracování prováděných pro Objednatele podle čl. 30 GDPR;

   7.5. nezapojit do zpracování žádného dalšího zpracovatele (krom poddodavatelů uvedených v příloze této Smlouvy za podmínek stanovených touto Smlouvou a v nezbytně nutném rozsahu) bez předchozího konkrétního nebo obecného písemného povolení Objednatele;

   7.6. pokud Poskytovatel zapojí jakéhokoliv dalšího zpracovatele (včetně poddodavatelů uvedených v příloze této smlouvy), budou tomuto dalšímu zpracovateli na základě samostatné smlouvy uzavřené mezi Poskytovatelem a tímto zpracovatelem uloženy stejné povinnosti na ochranu údajů, jaké jsou uvedeny v této smlouvě, a to zejména v tomto článku;

   7.7. při zohlednění povahy zpracování být Objednateli nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění Objednatelovy povinnosti reagovat na žádosti o výkon práv subjektů údajů;

   7.8. být při zohlednění povahy zpracování a informací, jež má Poskytovatel k dispozici, Objednateli nápomocen při zajišťování souladu s povinnostmi Objednatele: (i) zajistit dostatečnou úroveň zabezpečení zpracování ve smyslu čl. 32 GDPR, (ii) ohlašovat

případy porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů a případně též subjektům údajů ve smyslu čl. 33 a čl. 34 GDPR, (iii) posuzovat vliv na ochranu osobních údajů ve smyslu čl. 35 GDPR a (iv) v případě potřeby realizovat předchozí konzultace s Úřadem pro ochranu osobních údajů ve smyslu čl. 36 GDPR;

7.9. v souladu s rozhodnutím Objednatele všechny Osobní údaje buď vymazat, nebo vrátit objednateli po ukončení poskytování plnění dle této Smlouvy, a vymazat existující kopie, pokud právo Evropské unie nebo členského státu nepožaduje uložení daných Osobních údajů;

7.10. poskytnout Objednateli veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené POOÚ; a

7.11. umožnit audity, včetně inspekcí, prováděné Objednatelem nebo jiným auditorem, kterého Objednatel pověřil, a k těmto auditům přispívat.

8. Poskytovatel prohlašuje, že přijal a bude po celou dobu trvání této Smlouvy udržovat taková technická a organizační opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k Osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití Osobních údajů. Poskytovatel prohlašuje, že přijal a bude udržovat minimálně následující opatření k zajištění přiměřené úrovně zabezpečení:

8.1. pseudonymizace nebo šifrování osobních údajů;

8.2. schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování – zavedená opatření a jejich korektní fungování budou pravidelně kontrolovány;

8.3. schopnost obnovit dostupnost Osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;

8.4. proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování;

8.5. přístup k Osobním údajům mají výhradně oprávnění zaměstnanci nebo pracovníci Poskytovatele vázaní povinností mlčenlivosti, kteří mají přístup k Osobním údajům pouze v rozsahu odpovídajícím oprávnění těchto osob a kteří byli poučeni o povoleném způsobu nakládání s Osobními údaji.

Při posuzování vhodné úrovně bezpečnosti a přiměřenosti výše uvedených opatření se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných Osobních údajů, nebo neoprávněný přístup k nim.

9. V případě, že Poskytovatel zjistí porušení zabezpečení osobních údajů, ohlásí je okamžitě, nejpozději však do 24 hodin od takového zjištění, Objednateli. Nápravu je zhotovitel povinen zajistit do 48 hodin od zjištění porušení zabezpečení osobních údajů.

10. V případě ukončení této Smlouvy nejsou Poskytovatel, resp. jeho zaměstnanci, popř. jím pověřené třetí osoby, které přišly do styku s Osobními údaji dle výše uvedených ustanovení tohoto článku, zbaveni mlčenlivosti. Povinnost mlčenlivosti u nich v takovémto případě trvá i po ukončení účinnosti této Smlouvy, bez ohledu na trvání pracovního či jiného obdobného poměru uvedených osob k Poskytovateli.

XV. SANKCE A NÁHRADA ŠKODY

1. Smluvní strany se dohodly, že:

1.1. v případě nedodržení doby reakce v režimu 24x7 dle SLA uvedených v Příloze č. 1 se Poskytovatel zavazuje uhradit Objednateli smluvní pokutu ve výši 2 500,- Kč za každou započatou hodinu prodlení s dobou reakce, a to při každém porušení povinnosti;

1.2. v případě nedodržení doby vyřešení v režimu 24x7 dle SLA uvedených v Příloze č. 1 se Poskytovatel zavazuje uhradit Objednateli smluvní pokutu ve výši 2 500,- Kč za každou započatou hodinu prodlení s dobou vyřešení, a to při každém porušení povinnosti;

1.3. v případě prodlení s doručením Nabídky dle čl. VIII. odst. 2.2. Smlouvy se Poskytovatel zavazuje uhradit Objednateli smluvní pokutu ve výši 1 000,- Kč za každý započatý den prodlení;

1.4. v případě prodlení s poskytnutím plnění ze Služeb na objednávku se Poskytovatel zavazuje uhradit Objednateli smluvní pokutu ve výši 2 000,- Kč za každý započatý den prodlení;

1.5. v případě prodlení s odstraněním vytknuté vady, výhrady či připomínky v souladu s Protokolem o akceptačním řízení dle čl. VIII. odst. 7.5. Smlouvy se Poskytovatel zavazuje uhradit Objednateli smluvní pokutu ve výši 1 000,- Kč za každý započatý den prodlení.

2. Poruší-li Poskytovatel jakoukoliv povinnost podle čl. XIII. odst. 1. nebo 2. nebo čl. XIX. odst. 13. až 15. nebo čl. XXI. odst. 1. až 7. Smlouvy, je povinen uhradit Objednateli smluvní pokutu ve výši 10 000,- Kč za každé jednotlivé porušení.

3. Poruší-li Poskytovatel jakoukoliv povinnost podle čl. IX. odst. 3. až 40. Smlouvy (vyjma odst. 8., 9., 20. až 21. a 25. Smlouvy), je povinen uhradit Objednateli smluvní pokutu ve výši 10 000,- Kč za každé jednotlivé porušení.

4. Pokud Poskytovatel poruší povinnost či prohlášení dle čl. X. odst. 12. Smlouvy, vzniká Objednateli nárok na smluvní pokutu ve výši 2 000 000,- Kč za každý jednotlivý případ takového porušení.

5. Pokud Poskytovatel poruší povinnost dle čl. IX. odst. 25. Smlouvy, je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 50 000,- Kč za každé jednotlivé porušení povinnosti.

6. Pokud Poskytovatel poruší jakoukoliv povinnost dle čl. XVII. odst. 2. až 4. Smlouvy, je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 150 000,- Kč za každé jednotlivé porušení povinnosti.

7. Pokud Poskytovatel poruší své povinnosti stanovené POOÚ a/nebo touto Smlouvou, zejména povinnosti uvedené v čl. XIV. odst. 7. až 10. této Smlouvy, je povinen uhradit smluvní pokutu ve výši 500 000,- Kč za každé jednotlivé porušení.

8. Zaplacení smluvní pokuty nezbavuje Poskytovatele povinnosti splnit dluh smluvní pokutou utvrzený.

9. Objednatel je oprávněn požadovat náhradu škody a nemajetkové újmy způsobené porušením povinnosti Poskytovatele, na kterou se vztahuje smluvní pokuta, v plné výši.

10. Smluvní strany mají povinnost k náhradě škody v rámci platných a účinných právních předpisů a Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.

11. Žádná ze Smluvních stran neodpovídá za škodu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé Smluvní strany. V případě, že Objednatel poskytl Poskytovateli chybné zadání a Poskytovatel s ohledem na svou povinnost poskytnout Služby s odbornou péčí mohl nebo měl chybnost takového zadání zjistit, smí se ustanovení předchozí věty dovolávat pouze v případě, že na chybné zadání Objednatele písemně upozornil a Objednatel trval na původním zadání.

12. Žádná ze Smluvních stran nemá povinnost nahradit škodu způsobenou porušením svých povinností vyplývajících z této Smlouvy, bránila-li jí v jejich splnění některá z překážek vylučujících povinnost k náhradě škody ve smyslu § 2913 odst. 2 Občanského zákoníku. Smluvní strana, u níž nastala okolnost vylučující povinnost k náhradě škody, je povinna o této skutečnosti neprodleně písemně informovat druhou Smluvní stranu. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání těchto okolností vylučujících odpovědnost.

13. Poskytovatel prohlašuje, že veškeré výstupy Služeb poskytnutých podle této Smlouvy budou prosté právních vad a zavazuje se nahradit v plné výši Objednateli škodu v případě, že třetí osoba úspěšně uplatní autorskoprávní nebo jiný nárok plynoucí z právní vady poskytnutých výstupů Služeb. V případě, že by nárok třetí osoby vzniklý v souvislosti se Službami, bez ohledu na jeho oprávněnost, vedl k dočasnému či trvalému soudnímu zákazu či omezení užívání výstupu Služeb či jeho části, zavazuje se Poskytovatel zajistit náhradní řešení a minimalizovat dopady takovéto situace, a to bez dopadu na cenu Služeb sjednanou podle této Smlouvy, přičemž současně nebudou dotčeny ani nároky Objednatele na náhradu škody.

14. Žádná ze Smluvních stran není odpovědná za prodlení způsobené prodlením s plněním povinností druhou Smluvní stranou.

15. Nahrazuje se skutečná škoda a ušlý zisk. Náhrada škody se řídí obecnými ustanoveními Občanského zákoníku upravujícími náhradu škody.

16. Uplatněním nebo zaplacením smluvní pokuty či slev z ceny není dotčeno ani omezeno právo poškozené Smluvní strany na náhradu škody.

17. Náhrada škody se platí v měně platné na území České republiky.

XVI. TRVÁNÍ SMLOUVY A JEJÍ UKONČENÍ

1. Smlouva se uzavírá na dobu neurčitou.

2. Smlouva může být před uplynutím doby, na kterou byla sjednána, ukončena:

   2.1. odstoupením za podmínek stanovených touto Smlouvou; nebo

   2.2. výpovědí za podmínek stanovených touto Smlouvou; nebo

   2.3. dohodou Smluvních stran.

3. Poskytovatel je oprávněn od této Smlouvy odstoupit pouze v případě jejího podstatného porušení Objednatelem, které nebude napraveno ani do šedesáti (60) dnů ode dne doručení písemné výzvy k nápravě Objednateli.

4. Objednatel je oprávněn od Smlouvy odstoupit z důvodů stanovených právními předpisy nebo sjednaných Smlouvou. Objednatel je oprávněn odstoupit od Smlouvy zejména:

   4.1. v případě nedodržení sledovaných parametrů SLA u Průběžně poskytovaných Služeb majících za následek vznik povinnosti Poskytovatele zaplatit Objednateli smluvní pokutu ve výši minimálně 50 000,- Kč ve dvou po sobě jdoucích kalendářních měsících;

   4.2. jestliže celková výše smluvních pokut, na jejichž zaplacení vznikne Objednateli dle této Smlouvy nárok, přesáhne 1 000 000,- Kč;

   4.3. ukáže-li se jako nepravdivé jakékoliv prohlášení Poskytovatele uvedené ve Smlouvě;

   4.4. ocitne-li se Poskytovatel ve stavu úpadku nebo hrozícího úpadku;

   4.5. jestliže Poskytovatel bezdůvodně přeruší poskytování některé ze Služeb;

   4.6. jestliže Poskytovatel poruší některou svoji povinnost uvedenou v čl. XIII. odst. 1. nebo 2. čl. XXI. odst. 1. až 7. Smlouvy;

   4.7. poruší-li Poskytovatel jakoukoliv povinnost dle Smlouvy podstatným způsobem;

   4.8. bude-li Poskytovatel pravomocně odsouzen za trestný čin uvedený v příloze č. 3 Zákona o zadávání veřejných zakázek;

   4.9. bude-li Poskytovateli uložen zákaz plnění veřejných zakázek;

   4.10. v případě významné změny ovládání Poskytovatele dle ZOK nebo významné změny kontroly nad Poskytovatelem, nebo změny vlastnictví zásadních aktiv, využívaných Poskytovatelem k plnění podle Smlouvy, popřípadě změny oprávnění nakládat s těmito aktivy nebo změny kontroly nad nimi.

5. Smluvní strany jsou oprávněny tuto Smlouvu bez uvedení důvodů vypovědět, a to i z části, tzn. ve vztahu k jednotlivým modulům pracovišť komplementu, a to nejdříve po 18 měsících ode dne zahájení poskytování Služeb dle této Smlouvy. V případě Objednatele činí výpovědní doba 3 měsíce a počíná běžet prvního dne měsíce následujícího po doručení výpovědi Poskytovateli. V případě Poskytovatele činí výpovědní doba 12 měsíců a počíná běžet prvního dne měsíce následujícího po doručení výpovědi Objednateli.

XVII. EXIT

1. Poskytovatel se zavazuje dle pokynů Objednatele poskytnout veškerou potřebnou součinnost, dokumentaci a informace, účastnit se jednání s Objednatelem a popřípadě se třetími osobami za účelem plynulého a řádného převedení všech činností spojených s poskytováním Služeb, dojde-li k ukončení této Smlouvy (dále jen „***Exit***“).

2. Za tímto účelem se Poskytovatel zavazuje ve lhůtách dle odst. 3 tohoto článku Smlouvy vypracovat na základě pokynu Objednatele dokumentaci vymezující způsob provedení Exitu, odpovídající analýzu rizik, jejich zhodnocení a návrh jejich eliminace, harmonogram činností a jednotlivých kroků (dále jen „***Exitový plán***“), a poskytnout plnění nezbytná k realizaci tohoto Exitového plánu za přiměřeného použití vhodných ustanovení této Smlouvy.

3. Objednatel je oprávněn požádat o vypracování Exitového plánu ihned poté, jakmile zjistí, že Smlouva bude ukončena, tj. kdykoli spolu s odstoupením Objednatele či Poskytovatele od této Smlouvy, nebo i po takovém odstoupení, popřípadě kdykoli spolu s výpovědí Smlouvy Objednatelem či Poskytovatelem, nebo i po takové výpovědi. Poskytovatel se zavazuje vypracovat Exitový plán a poskytnout plnění nezbytná k jeho realizaci do 1 měsíce od doručení takového požadavku Objednatele, nestanoví-li Objednatel lhůtu delší. Vypracováním Exitového plánu se rozumí jeho schválení Objednatelem v souladu s tímto článkem Smlouvy.

4. V případě jakéhokoliv ukončení Smlouvy je Poskytovatel na základě Exitového plánu povinen poskytnout Objednateli nebo Objednatelem určené třetí osobě plnění a maximální nezbytnou součinnost za účelem:

   4.1. plynulého a řádného převedení činností dle Smlouvy či jejich části na Objednatelem určenou třetí osobu, s výjimkou případu, že by novým poskytovatelem Služeb byl Poskytovatel dle této Smlouvy, tak, aby Objednateli nevznikla újma (škoda) související s přechodem poskytování plnění dle této Smlouvy na nového poskytovatele Služeb nebo

   4.2. plynulého a řádného předání všech dat souvisejících se Systémem Objednateli nebo Objednatelem určené třetí osobě, v takové podobě, způsobem a tak, aby Objednatel nebo Objednatelem určená třetí osoba byli schopni řádně provozovat nový systém nahrazující Systém dle této Smlouvy.

   Poskytovatel se zavazuje tato plnění a maximálně nezbytnou součinnost poskytovat s odbornou péčí, zodpovědně v rozsahu, který po něm lze spravedlivě požadovat, a to do doby úplného převzetí takových činností Objednatelem určenou třetí osobou nebo převzetí takových dat Objednatelem nebo Objednatelem určenou třetí osobou. Součinnost bude spočívat především ve vykonání plánu předání (dle Exitového plánu činnostmi vedoucími k řádnému vykonání Exitového plánu).

5. Smluvní strany se dohodly, že cena za vypracování Exitového plánu a poskytnutí plnění nezbytného k jeho realizaci vedoucího k úspěšnému Exitu či poskytování další součinnosti dle tohoto článku Smlouvy je součástí Ceny Služeb.

6. Smluvní strany se dohodly, že v případě sporu o jakékoli otázce, která se týká Exitového plánu dle tohoto článku Smlouvy, může být jejich dohodou určen soudní znalec pro posouzení sporné otázky a Smluvní strany se budou takovým posouzením soudního znalce řídit.

7. V případě, že není možné povinnosti uvedené v tomto článku této Smlouvy splnit před okamžikem zániku smluvního závazkového vztahu založeného touto Smlouvu z důvodu, že tento okamžik není předem znám (například v případě odstoupení), zkracují se lhůty uvedené v předchozích odstavcích tohoto článku této Smlouvy na polovinu, začínají plynout až od okamžiku zániku smluvního závazkového vztahu založeného touto Smlouvu a taktéž příslušné povinnosti budou plněny až po okamžiku zániku smluvního závazkového vztahu založeného touto Smlouvu.

8. Poskytovatel bere na vědomí a uznává, že v případě neposkytnutí jeho součinnosti dle tohoto článku XVI. této Smlouvy může Objednateli vzniknout škoda z důvodu nemožnosti nebo ztížené možnosti zadat poskytování Služeb nebo služeb podobným Službám či s nimi jinak spojených novému poskytovateli nebo nemožnosti nebo ztížené možnosti řádně provozovat nový systém nahrazující Systém dle této Smlouvy. Poskytovatel bere dále na vědomí a uznává, že v případě neposkytnutí jeho součinnosti dle tohoto článku XVI. této Smlouvy může dojít k omezení možnosti Objednatele poskytovat služby zdravotní péče a Objednatel bude ekonomické dopady takového omezení jeho možnosti poskytovat služby zdravotní péče považovat za škodu dle této Smlouvy vzniklou z důvodu neposkytnutí součinnosti Poskytovatele dle tohoto článku XVI. této Smlouvy.

9. Nad rámec povinností dle tohoto článku XVII., za jejichž splnění nenáleží Poskytovateli další odměna nad rámec ceny za Průběžně poskytované Služby za dobu jejich poskytování dle této Smlouvy, je Poskytovatel povinen až do uplynutí šesti (6) měsíců od zániku smluvního závazkového vztahu založeného touto Smlouvou poskytovat Objednateli jakékoliv další konzultace související s provozem Sytému. Za konzultace dle předchozí věty náleží Poskytovateli odměna ve výši vycházející ze sjednaných sazeb za Služby na objednávku.

XVIII. PROHLÁŠENÍ SMLUVNÍCH STRAN

1. Poskytovatel prohlašuje, že není v úpadku ani ve stavu hrozícího úpadku, a že mu není známo, že by vůči němu bylo zahájeno insolvenční řízení. Poskytovatel dále prohlašuje, že vůči němu není v právní moci žádné soudní rozhodnutí, případně rozhodnutí správního, daňového či jiného

orgánu na plnění, které by mohlo být důvodem zahájení exekučního řízení na majetek Poskytovatele a že mu není známo, že by vůči němu takové řízení bylo zahájeno.

2. Poskytovatel na sebe přebírá nebezpečí změny okolností ve smyslu § 1765 Občanského zákoníku.

3. Vzhledem k veřejnoprávnímu charakteru Objednatele Poskytovatel výslovně prohlašuje, že je s touto skutečností obeznámen a souhlasí se zveřejněním Smlouvy v rozsahu a za podmínek vyplývajících z příslušných právních předpisů.

4. Poskytovatel si je vědom, že je ve smyslu § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, povinen spolupůsobit při výkonu finanční kontroly.

5. Smluvní strany prohlašují, že identifikační údaje uvedené v záhlaví této Smlouvy odpovídají aktuálnímu stavu a že osobami jednajícími při uzavření Smlouvy jsou osoby oprávněné k jednání za Smluvní strany bez jakéhokoliv omezení vnitřními předpisy Smluvních stran.

6. Jakékoliv změny údajů uvedených v záhlaví této Smlouvy, jež nastanou v době po uzavření Smlouvy, jsou Smluvní strany povinny bez zbytečného odkladu písemně sdělit druhé Smluvní straně.

7. V případě, že se kterékoliv prohlášení některé ze Smluvních stran uvedené ve Smlouvě ukáže býti nepravdivým, odpovídá tato Smluvní strana za škodu a nemajetkovou újmu, které nepravdivostí prohlášení nebo v souvislosti s ní druhé Smluvní straně vznikly.

XIX. OSTATNÍ UJEDNÁNÍ

1. Tvoří-li Poskytovatele více osob, platí následující:

   1.1. všechny osoby tvořící Poskytovatele jsou ze Smlouvy zavázány společně a nerozdílně,

   1.2. jednání kterékoli z osob tvořících Poskytovatele je přičítáno Poskytovateli bez ohledu na vnitřní vztahy mezi jednotlivými osobami tvořícími Poskytovatele,

   1.3. za Poskytovatele může jednat kterákoli z osob tvořících Poskytovatele.

2. Poskytovatel je povinen neprodleně písemně informovat Objednatele o skutečnostech majících i potenciálně vliv na plnění jeho povinností vyplývajících ze Smlouvy, a není-li to možné, nejpozději následující den poté, kdy příslušná skutečnost nastane nebo Poskytovatel zjistí, že by nastat mohla. Současně je Poskytovatel povinen učinit veškeré nezbytné kroky vedoucí k eliminaci případné škody hrozící Objednateli, a to zejména obstarat neprodleně náhradní plnění, přičemž je povinen nést případný rozdíl ceny.

3. Poskytovatel bere na vědomí, že Objednatel je povinným subjektem podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

4. Smlouva je platná dnem připojení platného uznávaného elektronického podpisu dle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů, oběma Smluvními stranami do této Smlouvy a jejích jednotlivých příloh, nejsou-li součástí jediného elektronického dokumentu (tj. do všech samostatných souborů tvořících v souhrnu Smlouvu).

5. Tato Smlouva nabývá účinnosti dnem uveřejnění v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů (dále jen „***Zákon o registru smluv***“). Poskytovatel souhlasí se zveřejněním Smlouvy v souladu s povinnostmi Objednatele za podmínek vyplývajících z příslušných právních předpisů, zejména souhlasí se zveřejněním Smlouvy, včetně všech jejích změn a dodatků, výše skutečně uhrazené ceny na základě Smlouvy a dalších údajů na profilu zadavatele Objednatele podle Zákona o zadávání veřejných zakázek a v registru smluv podle Zákona o registru smluv. Smluvní strany se dohodly, že zákonnou povinnost dle § 5 odst. 2 Zákona o registru smluv splní Objednatel. Poskytovatel prohlašuje, že Smlouva ani žádná její část nejsou obchodním tajemstvím Poskytovatele ve smyslu § 504 Občanského zákoníku.

6. Poskytovatel je povinen chránit osobní údaje a při jejich ochraně postupovat v souladu s příslušnými právními předpisy, zejména se zákonem č. 110/2019 Sb., o zpracování osobních údajů, v platném znění. Poskytovatel je povinen dodržovat podle Nařízení evropského parlamentu a rady (EU) 2016/679 ze dne 27.04.2016 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), povinnost zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Poskytovatel je dále povinen zajistit, aby osobní údaje pacientů Objednatele a dalších osob (zaměstnanců Objednatele nebo dodavatelů Objednatele), jakož i veškeré informace, které se Poskytovatel v průběhu Řízení veřejné zakázky, jakož i v průběhu plnění závazků vyplývajících z této Smlouvy dozví o činnosti, struktuře a IT prostředí Objednatele neopustila sídlo a prostředí Objednatele.

7. Poskytovatel se zavazuje zachovávat mlčenlivost o všech skutečnostech, o nichž se dozví u Objednatele při plnění závazků dle této Smlouvy nebo v souvislosti s ní. To platí zejména o skutečnostech, na něž se vztahuje povinnost mlčenlivosti zdravotnických pracovníků, zejména podle ustanovení § 51 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů.

8. Poskytovatel není oprávněn postoupit žádnou svou pohledávku za Objednatelem vyplývající ze Smlouvy nebo vzniklou v souvislosti se Smlouvou ani postoupit Smlouvu nebo její část bez předchozího písemného souhlasu Objednatele s postoupením.

9. Poskytovatel není oprávněn provést jednostranné započtení žádné své pohledávky za Objednatelem vyplývající ze Smlouvy nebo vzniklé v souvislosti se Smlouvou na jakoukoliv pohledávku Objednatele za Poskytovatelem bez předchozího písemného souhlasu Objednatele se započtením.

10. Objednatel je oprávněn provést jednostranné započtení jakékoliv své splatné i nesplatné pohledávky za Poskytovatelem vyplývající ze Smlouvy nebo vzniklé v souvislosti se Smlouvou (zejména smluvní pokutu) na jakoukoliv splatnou i nesplatnou pohledávku Poskytovatele za Objednatelem.

11. Poskytovatel je povinen zachovávat mlčenlivost o všech skutečnostech a informacích, které jsou obsažené ve Smlouvě a dále o všech skutečnostech a informacích, které mu byly v souvislosti se Smlouvou nebo jejím plněním jakkoliv zpřístupněny, předány či sděleny, nebo o nichž se jakkoliv dozvěděl v souvislosti se Smlouvou, vyjma těch, které jsou v okamžiku, kdy se s nimi Poskytovatel seznámil, prokazatelně veřejně přístupné nebo těch, které se bez zavinění Poskytovatele veřejně přístupnými stanou. Poskytovatel nesmí takové skutečnosti a informace použít v rozporu s jejich účelem, nesmí je použít ve prospěch svůj nebo jiných osob a nesmí je použít ani v neprospěch Objednatele. Povinnosti podle tohoto odstavce je Poskytovatel povinen zachovávat i po zániku závazku ze Smlouvy, vyjma případů, kdy se takové skutečnosti a informace stanou prokazatelně veřejně přístupné bez zavinění Poskytovatele. Povinnosti podle tohoto odstavce se nevztahují na případy, kdy je Poskytovatel povinen zveřejnit takové skutečnosti nebo informace na základě povinnosti uložené mu právním předpisem nebo rozhodnutím orgánu veřejné moci.

12. Zánikem nebo ukončením této Smlouvy nejsou dotčena práva a povinnosti vyplývající z ustanovení této Smlouvy, která dle projevené vůle Smluvních stran nebo vzhledem ke své povaze mají trvat i po ukončení této Smlouvy, a to zejména práva a povinnosti související s odpovědností za škodu, náhradou škody, smluvními pokutami, fakturací cen, s úroky z prodlení, dále s licencí, odpovědností za vady, zárukou a ochranou osobních údajů a mlčenlivostí.

13. Poskytovatel se zavazuje zajistit důstojné pracovní podmínky, bezpečnost práce a dodržování veškerých pracovněprávních předpisů, zejména pak zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů (odměňování, pracovní doba, doba odpočinku mezi směnami, placené přesčasy) a zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a to vůči všem osobám, které se na plnění předmětu Smlouvy budou podílet a bez ohledu na to, zda bude plnění předmětu Smlouvy prováděno Poskytovatelem či jeho poddodavatelem.

14. Poskytovatel se zavazuje k dodržování veškerých povinností zaměstnavatele vztahujících se k jeho zaměstnancům a příslušným institucím a vyplývajících ze zákona č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů, ve znění pozdějších předpisů, zákona č. 592/1992 Sb., o pojistném na všeobecné zdravotní pojištění, ve znění pozdějších předpisů, a zákona č. 187/2006 Sb., o nemocenském pojištění, ve znění pozdějších předpisů.

15. Poskytovatel se zavazuje zachovávat férové vztahy v dodavatelsko-odběratelském řetězci, tj. zejména ve vztahu ke svým poddodavatelům. Jakýkoliv závazek uzavřený Poskytovatelem a jeho poddodavatelem, jehož předmětem je plnění (části) této Smlouvy, nesmí obsahovat splatnost faktury delší než 30 dnů.

16. Smluvní strany se zavazují, že budou v maximální možné míře zajišťovat digitalizaci jakýchkoliv úkonů, služeb a agend souvisejících se Systémem a poskytovanými službami. Smluvní strany v maximální možné míře upřednostní elektronickou komunikaci, a to i ve vztahu k fakturaci a platbám.

XX. ZMOCNĚNCI

1. Zmocněnci Smluvních stran jsou následující:

   Za Objednatele:

   pro jednání věcná a technická:

   Vedoucí Odboru informačních systémů;

   pro jednání o naplňování požadavků zákona o kybernetické bezpečnosti:

   Manažer kybernetické bezpečnosti.

   za Poskytovatele:

   pro jednání věcná a technická:

   Produktový manažer, Projektový manažer;

   pro jednání o naplňování požadavků zákona o kybernetické bezpečnosti:

   Manažer kvality a bezpečnosti.

2. Smluvní strany jsou oprávněny jednostranně změnit zmocněnce uvedené v odst. 1. tohoto článku Smlouvy bez nutnosti uzavření dodatku ke Smlouvě. V takovém případě jsou povinny na takovou změnu druhou Smluvní stranu předem písemně upozornit, jinak tato změna nemá vůči druhé Smluvní straně právní účinky.

XXI. PODDODAVATELÉ

1. Poskytovatel je oprávněn pověřit plněním svých povinností vyplývajících ze Smlouvy pouze jiné osoby uvedené v příloze č. 4 Smlouvy, nebo osoby písemně odsouhlasené Objednatelem (dále jen „***Příloha č. 4***“, uvedené osoby jednotlivě dále jen „***Poddodavatel***“ nebo společně „***Poddodavatelé***“).

2. Poskytovatel odpovídá za plnění Poddodavatele tak, jako by plnil sám. Objednatel je povinen vybírat Poddodavatele tak, aby Poddodavatelé nebyli v rozporu s požadavky Objednatele na Poskytovatele. Poskytovatel je povinen zavázat své Poddodavatele ve vztahu ke kyberbezpečnosti (tj. dle požadavků zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti) ve stejném rozsahu, v jakém je zavázán Poskytovatel vůči Objednateli, přičemž existenci takového závazku je povinen na vyžádání Objednatele bez zbytečného odkladu prokázat, a to např. předložením smlouvy uzavřené s příslušným Poddodavatelem.

3. Poskytovatel prohlašuje a zavazuje se, že jako ručitel uspokojí za jakéhokoliv Poddodavatele jeho povinnost nahradit újmu způsobenou Poddodavatelem Objednateli při plnění nebo v souvislosti s plněním povinností ze Smlouvy, jestliže Poddodavatel povinnost k náhradě újmy nesplní. Objednatel Poskytovatele jako ručitele podle předchozí věty přijímá.

4. Poskytovatel se zavazuje, že Poddodavatelé, kterými prokazoval splnění kvalifikace v Řízení veřejné zakázky, se budou podílet na plnění povinností Poskytovatele vyplývajících ze Smlouvy v rozsahu podle nabídky Poskytovatele podané do Řízení veřejné zakázky.

5. Objednatel je oprávněn požadovat a Poskytovatel je povinen zabezpečit změnu Poddodavatele nebo část Služeb prováděnou Poddodavatelem provést sám, splňuje-li všechny pro plnění příslušné části Služeb Objednatelem stanovené předpoklady a kvalifikaci, a to v případech, kdy:

   5.1. bude Poddodavatel vůči Objednateli v prodlení se splněním povinnosti z jiného závazku nebo

   5.2. bude Poddodavatel pravomocně odsouzen za trestný čin uvedený v příloze č. 3 Zákona o zadávání veřejných zakázek nebo

   5.3. se Poddodavatel ocitne ve stavu úpadku nebo hrozícího úpadku nebo

   5.4. bude Poddodavateli uložen zákaz plnění veřejných zakázek nebo

5.5. bude dán jiný závažný důvod pro změnu Poddodavatele (např. důvod obdobný důvodu pro odstoupení Objednatele od Smlouvy).

6. Poskytovatel je povinen navrhnout nového Poddodavatele do 10 dnů od doručení žádosti Objednatele. Nový Poddodavatel může být připuštěn k plnění Služeb výlučně na základě písemného souhlasu Objednatele.

7. Poskytovatel je oprávněn změnit Poddodavatele z důvodů na straně Poskytovatele pouze s předchozím písemným souhlasem Objednatele. Objednatel vydá písemný souhlas se změnou do 10 dnů od doručení žádosti Poskytovatele. Objednatel souhlas se změnou nevydá, pokud:

7.1. prostřednictvím původního Poddodavatele Poskytovatel v Řízení veřejné zakázky prokazoval splnění kvalifikace a nový Poddodavatel nebude mít stejnou či vyšší kvalifikaci, než jaká byla stanovena v Řízení veřejné zakázky nebo

7.2. po Objednateli nelze spravedlivě požadovat, aby s takovou změnou souhlasil.

XXII. ZÁVĚREČNÁ USTANOVENÍ

1. Přílohy Smlouvy jsou její nedílnou součástí. V případě rozporu znění přílohy Smlouvy a Smlouvy se použije přednostně znění Smlouvy.

2. Veškerá práva a povinnosti Smluvních stran vyplývající ze Smlouvy se řídí českým právním řádem. Smluvní strany se dohodly, že ustanovení právních předpisů, která nemají donucující účinky, mají přednost před obchodními zvyklostmi a zavedenou praxi Smluvních stran, pokud Smlouva nestanoví jinak.

3. Všechny spory vznikající ze Smlouvy a v souvislosti s ní budou řešeny především dohodou Smluvních stran, přičemž nedojde-li k dohodě o řešení sporů, budou tyto podle vůle Smluvních stran rozhodovány soudy České republiky, jakožto soudy výlučně příslušnými.

4. Smlouvu lze měnit pouze písemnými, vzestupně číslovanými dodatky, pokud Smlouva nestanoví jinak. Jakékoli změny Smlouvy učiněné jinou než písemnou formou jsou vyloučeny.

5. Tato Smlouva se vyhotovuje v elektronické podobě, přičemž obě Smluvní strany obdrží její elektronický originál.

6. Ukončením Smlouvy nejsou dotčeny Objednávky a Nabídky, pokud se Smluvní strany nedohodnou jinak.

7. Smlouva nabývá platnosti dnem jejího uzavření. Smlouva nabývá účinnosti uveřejněním v registru smluv dle Zákona o registru smluv.

PŘÍLOHY:

Příloha č. 1	Katalog služeb
Příloha č. 2	Popis AS-IS stavu
Příloha č. 3	Ceník Služeb
Příloha č. 4	Poddodavatelé
Příloha č. 5	Metodika řízení dodavatelů
Příloha č. 6	Nástroj pro hodnocení dodavatele dle VKB
Příloha č. 7	Zachování kontinuity podpory
Příloha č. 8	Metodika hodnocení rizik

V Praze dne *datum viz elektronický podpis*

[redacted] Datum: 2023.07.14 11:39:59 +02'00'

.....

za Objednatele

[redacted] Fakultní nemocnice v Motole

V Praze dne *datum viz elektronický podpis*

[redacted]

.....

za Poskytovatele

[redacted]

Příloha č. 1 Smlouvy

Katalog služeb

Servisní podpora

Servisní podpora (dále jen ***„Servisní podpora“***) bude Poskytovatelem poskytována v níže uvedeném
rozsahu.

Technická podpora

Poskytovatel je povinen zajistit Objednateli možnost využívat technické podpory, a to prostřednictvím těchto nástrojů:

	Nástroj	**Dostupný na**
a)	**Online helpdeskový systém**	
b)	**Telefonická hotline**	Servicedesk (8x5): Hotline (24x7): • Laboratoře, RDG - • Transfuzní oddělení - • Chorobopis - • Produktový manažer:
c)	**E-mail**	**1. laboratoř biochemie, hematologie, imunologie, laboratoř mikrobiologie, laboratoř toxikologie, centrální příjem biologického materiálu:** **2. laboratoř patologie + Perseus:** **3. laboratoř transfuzní, transfúzní oddělení, skládek:** **4. radiodiagnostické pracoviště:** **5. chorobopis, účtování**

Poskytovatel je v rámci technické podpory povinen pro Objednatele za dále v této příloze uvedených podmínek zejména:

- přijímat oznámení o vadách Systému a oznamovat průběh jejich řešení,
- přijímat Požadavky na školení, konzultace a další služby k Systému a na rozvoj Systému,
- poskytovat Objednateli uživatelskou podporu související s provozem Systému, tj. zodpovídat dotazy uživatelů apod.

Poskytovatel je povinen zajistit dostupnost těchto nástrojů nepřetržitě (tj. 24 hodin denně, 7 dní v týdnu, 365 (366) dní v roce).

Průběžné vyhodnocování provozu Systému, profylaxe Systému

Poskytovatel je za účelem předcházení vad Systému a za účelem zjištění bezpečnosti a optimálního provozu Systému povinen provádět průběžné vyhodnocování provozu Systému a dále je povinen provádět profylaxe Systému.

Poskytovatel je v rámci vyhodnocování provozu Systému povinen provádět měsíční analýzy provozu, a to:

- Systému včetně komunikace s dalšími propojenými systémy,
- databázového prostředí Systému,
- softwarové části replikačního serveru Systému.

Poskytovatel je povinen profylaxi Systému provádět 1x ročně po dobu trvání Smlouvy. Předmětem profylaxe Systému jsou zejména:

- kontrola vazeb (konzistence dat),
- zaplňování databázového prostoru a návrhy jeho rozšiřování,
- kontrola zálohování a bezpečnosti dat,
- mapování vytížení Systému a návrh optimalizace (zejména selekty a indexy).

Poskytovatel je na základě vyhodnocování provozu Systému a provádění profylaxí Systému povinen navrhnout a poskytnout součinnost při činnostech potřebných k optimalizaci provozu Systému a k předcházení poruch Systému a dále vypracovávat a Objednateli předkládat návrhy na zlepšení Systému a na zlepšení jeho využívání ze strany Objednatele (např. návrhy na opětovné proškolení uživatelů Systému, na organizační opatření Objednatele, na posílení, doplnění či přesun hardwarového vybavení, na kterém je Systém provozován apod.).

Poskytovatel je o provedené profylaxi povinen vyhotovit zápis a předat jej do 5 pracovních dní ode dne provedení profylaxe kontaktní osobě Objednatele.

V případě, že výsledky profylaxe ukáží na potřebu provedení rozvoje Systému, předloží Poskytovatel návrh takového řešení včetně odhadovaného časového rozsahu pracnosti v hodinách Objednateli.

Odstraňování vad Systému

Poskytovatel je za účelem zajištění odstraňování vad Systému povinen zajistit nepřetržitý příjem oznámení o vadách Systému s využitím Online helpdeskového systému.

V oznámení vady musí být vada popsána a musí být vymezena její závažnost. Objednatel je zároveň za účelem další domluvy a urychlení odstranění vady oprávněn Poskytovatele kontaktovat prostřednictvím Telefonické hotline.

Definice pojmů

Nad rámec pojmů s velkými počátečními písmeny definovanými ve Smlouvě s významem, který je jim připisován se použijí i pojmy s následujícím významem:

Doba reakce – jde o časovou lhůtu, ve které je Poskytovatel povinen odpovědět na jakoukoliv vadu Systému, která byla Objednatelem předána prostřednictvím příslušných nástrojů.

Doba vyřešení – u vad Systému jde o časovou lhůtu, ve které je Poskytovatel povinen jakoukoliv vadu zcela odstranit.

Vady jsou dle závažnosti členěny do tří kategorií:

Kategorie vady		**Definice závažnosti Závad a Chyb**
A	**Havárie**	Některé nebo všechny části Systému selhaly a jsou zcela nefunkční nebo je jejich funkčnost omezena tak, že je kritickým či zásadním způsobem ovlivněna činnost/funkčnost.
B	**Incident**	Stav Systému nebo jeho části, ve kterém jeho nějaká část není plně funkční či nefunguje ve standardním režimu.

C	**Omezení**	Systém není ve stavu Havárie či Incidentu. Systém je plně operativní, přičemž nefunkční část nemá podstatný vliv na činnost/funkčnost Systému nebo ji lze dočasně nahradit.

V případě sporu o zařazení vady v rámci kategorie je směrodatné zařazení ze strany Objednatele.

Provozní doba – doba, kdy je služba či její část poskytována – od-do, které dny v týdnu:

- **24x7** – nepřetržitě

Provozní parametry servisní podpory Systému:

Parametr	**Hodnota**
Provozní doba Telefonické hotline	Minimálně 8 hodin v pracovní dny, dle standardní pracovní doby Poskytovatele (musí být v časovém rozmezí 7:00 – 18:00 SEČ)
Provozní doba Online helpdeskového systému	24x7
Doba reakce na A v režimu 24x7	1 hodina
Doba vyřešení A v režimu 24x7	8 hodin
Doba reakce na B v režimu 24x7	1 hodina
Doba vyřešení B v režimu 24x7	120 hodin
Doba reakce na C v režimu 24x7	24 hodin
Doba vyřešení C v režimu 24x7	240 hodin
Doba pro údržbu služby v režimu 24x7	Po předchozí dohodě každé 3. pondělí v měsíci v době od 0:30 do 3:30

Poskytovatel je povinen bez zbytečného prodlení informovat Objednatele prokazatelným způsobem o zahájení prací na odstranění vady. Oznámením Poskytovatele o způsobu řešení se rozumí zápis konkrétní informace do Online helpdeskového systému.

Lhůta pro odstranění vady se prodlužuje o dobu poskytování nutné součinnosti ze strany Objednatele (např. doba reinstalace serveru, dodání a zprovoznění náhradních serverů a hardwarových komponent, hledání a kopírování záloh, zprovozňování souvisejících aplikací nedodaných Poskytovatelem).

V případě, že v průběhu odstraňování vady dojde ke změně kategorie vady směrem k nižší závažnosti (potvrzené Objednatelem), prodlužuje se lhůta pro odstranění vady na délku vztahující se k vadě této kategorie (i nová lhůta se však počítá od nahlášení vady). Toto prodloužení nemá vliv na již vzniklé prodlení a související povinnost uhradit smluvní pokutu.

Po odstranění vady Objednatel potvrdí odstranění vady v Online helpdeskovém systému. Tímto se vada považuje za odstraněnou.

Smluvní strany se dohodly, že v případě, že to povaha vady umožní, budou vady odstraňovány za využití vzdáleného přístupu pomocí VPN.

Do této doby se nezapočítává doba poskytování nutné součinnosti ze strany Objednatele (např. doba reinstalaci serveru, dodání a zprovoznění náhradních serverů a hardwarových komponent, hledání a kopírování záloh, zprovozňování souvisejících aplikací nedodaných Poskytovatelem).

Poskytovatel je povinen zajistit, aby Online helpdeskový systém automaticky u každé z nahlášených vad zobrazoval mj. okamžik nahlášení vady, zahájení odstraňování vady a odstranění vady a dále aby Objednateli umožňoval export přehledu nahlášených vad s informacemi o kategorii vady, okamžiku nahlášení, okamžiku zahájení odstraňování vady a odstranění vady ve formátu txt / csv.

Upgrade a update Systému

Poskytovatel je povinen poskytovat Objednateli upgrade a update Systému (resp. jeho stávajících modulů), tedy zlepšení a dodatky k Systému a jeho funkcionalitám vydaných Poskytovatelem, a to včetně vlastní instalace a implementace u Objednatele, dodání souvisejících licencí.

Poskytovatel je povinen provádět upgrade a update proprietárního softwaru tak, aby byla zajištěna bezpečnost tohoto softwaru a zároveň aby vždy byl Systém s touto novou verzí kompatibilní.

Poskytovatel tak není povinen zajistit vždy nejnovější verzi proprietárního softwaru, avšak vždy se musí jednat o vydavatelem tohoto proprietárního softwaru podporovanou verzi. Po dohodě s Objednatelem může být konkrétní proprietární software nahrazen jiným obdobným proprietárním softwarem, který zcela nahradí původní proprietární software.

Poskytovatel je v rámci updatu povinen instalovat hot-fixy a patche proprietárního softwaru.

Před provedením jednotlivých upgradů či updatů ze strany Poskytovatele musí vždy proběhnout odsouhlasení ze strany Objednatele (kontaktní osoby), a to minimálně v rozsahu prováděného upgradu či updatu a času jejich provádění.

Poskytovatel v souvislosti s poskytováním této Služby odpovídá také za zachování funkčních vazeb Systému na další systémy a databáze v souvislosti s poskytnutím této služby. V případě nedodržení, odpojení, narušení nebo jiné vady takových vazeb v souvislosti s poskytováním této služby se tyto vady považují za vady vysoké závažnosti – Havárie.

Legislativní podpora

Poskytovatel je prostřednictvím Služby Upgrade a update Systému povinen zajistit, aby byl Systém v souladu s právními předpisy (včetně předpisů Evropské unie).

V případě legislativních změn vyžadujících vytvoření zcela nového modulu Systému budou Smluvní strany postupovat dle podmínek pro Služby na objednávku.

Aktualizace číselníků

Poskytovatel se zavazuje provádět aktualizace číselníků Objednatele obsažených v Systému, a to bez prodlení po změně číselníku ze strany jeho poskytovatele.

Čtvrtletní rozvojová schůzka

Poskytovatel je povinen v sídle Objednatele po domluvě s Objednatelem každé čtvrtletí svolat schůzku, které se zúčastní fyzicky pověřený zaměstnanec Poskytovatele a klíčoví uživatelé na straně Objednatele. Předmětem schůzky bude podání zpětné vazby k fungování Systému a diskuse nad možnými zlepšeními a dalším rozvojem.

Napojování nových analyzátorů Objednatele na Systém

Poskytovatel se v rámci Služeb na objednávku zavazuje zajistit napojení nových analyzátorů Objednatele na Systém.

Podmínky poskytování této Služby se řídí ustanoveními Smlouvy o Službách na objednávku.

Další služby

Poskytovatel se v rámci Služeb na objednávku zavazuje Objednateli dále poskytovat zejména následující služby (dále také ***„Další služby“***):

- úprava dat softwaru,
- konfigurace softwaru (např. tvorba a úprava tiskových předloh (šablon), optimalizace komunikačních rozhraní),
- další služby obdobného charakteru a náročnosti k výše uvedeným službám,
- služby konzultační.

Podmínky poskytování Dalších služeb se řídí ustanoveními Smlouvy o Službách na objednávku.

Příloha č. 2 Smlouvy Popis AS-IS stavu

Systém: Moduly pracovišť komplementu

Moduly:

- laboratoř biochemie, hematologie, imunologie;
- laboratoř patologie;
- laboratoř mikrobiologie;
- laboratoř transfuzní;
- laboratoř toxikologie;
- centrální příjem biologického materiálu;
- radiodiagnostické pracoviště;
- transfúzní oddělení;
- skládek.

OBECNÝ POPIS

Systémy jsou v rámci prostředí FN Motol provozovány na OS Linux s SQL databázovým serverem Firebird. Programové vybavení využívá vlastnosti databázového SQL serveru formou uložených procedur, transakčního zabezpečení operací nad databází a možnosti on-line archivace za provozu. Klient systému je nainstalován na koncové stanici se systémem Windows (7, 10), se standardní tiskárnou, případně tiskárnou štítků.

Systémy jsou používány na většině pracovišť FN Motol. Počet definovaných uživatelů v systému UNIS ve FN Motol je 6000.

Systémy jsou členěny na moduly a koncipován tak, aby instalace systému na kterémkoliv pracovišti umožňovala provozovat libovolný modul podle potřeb pracoviště a oprávnění uživatelů FN Motol. V jednotlivých modulech jsou dostupné standardní společné funkcionality, které mohou být doplněny o další funkcionality dle specifických potřeb FN Motol. Uživatelské účty jsou definovány v systému a jsou přidělovány podle role a pracovního zařazení. K systémům je přístup pouze prostřednictvím počítačové sítě FN Motol.

Všechny moduly systémů musí být v souladu s platnou legislativou a ostatními souvisejícími předpisy v rámci výkonu zdravotní péče v FN Motol a to zejména výkaznictví vůči zdravotním pojišťovnám a dalším povinným subjektům.

Systémy jsou rozčleněny do standardních modulů, které obsahují standardní funkcionality pro příslušnou oblast léčebné péče a dále na moduly obsahující průřezové funkcionality. Některé moduly jsou doplněny specifickými funkcionalitami dle potřeb FN Motol. Jedná se o funkcionality zaměřené na integraci daných systémů s ostatními informačními systémy FN Motol, zdravotnickými či laboratorními přístroji a zařízeními nebo o funkcionality specifické pro prostředí FN Motol.

POPIS FUNKCÍ MODULŮ UNIS

V rámci FN MOTOL jsou využívány moduly UNIS a to:

- Chorobopis;
- Centrální modul UNIS;
- Účtárna;
- Moduly pracovišť komplementu;
- Transfuzní oddělení;
- Faktura;
- Žádanky.

Všechny součásti UNIS musí být v souladu s platnou legislativou a ostatními souvisejícími předpisy v rámci výkonu zdravotní péče v FN MOTOL a to zejména výkaznictví vůči zdravotním pojišťovnám a dalším povinným subjektům.

Popis modulů UNIS

Systém UNIS je rozčleněn do standardních modulů, které obsahují standardní funkcionality pro příslušnou oblast léčebné péče a dále na moduly obsahující průřezové funkcionality. Některé moduly jsou doplněny specifickými funkcionalitami dle potřeb FN MOTOL. Jedná se o funkcionality zaměřené na integraci UNIS s ostatními informačními systémy FN MOTOL, zdravotnickými či laboratorními přístroji a zařízeními nebo o funkcionality specifické pro prostředí FN MOTOL.

Modul Chorobopis

Modul Chorobopis obsahuje následující výčet funkcionalit:

- Vkládání pacientů – založení osobních dat;
- Lékařská dokumentace ambulantní a lůžkové části nemocnice;
- Záznamy o stavu a léčbě pacienta;
- Založení hospitalizace s příjmem, hlavičkou účtu, stravou a doprovodem pacienta;
- Sdílení lékařských zpráv z jiných pracovišť Zadavatele; MEDCENT;
- Generování a tisk receptů, poukazů na ortopedickou pomůcku, optických poukazů a žádanek o laboratorní vyšetření;
- E-neschopenka;
- E-očkování;
- Farmakokonzilium;
- Klasické konzilium;
- Dekurzy standardní a jipové vč. formalizované medikace;
- Elektronické žádanky o vyšetření na pracovištích komplementu;
- Objednávání pacientů dle časového fondu daného pracoviště – plánovací kalendáře pro zdravotnická pracoviště;
- Objednávání dle plánu zdrojů;
- Vedení účtů za zdravotní péči včetně metodiky DRG;
- Import laboratorních výsledků;
- Práce s obrazovou dokumentací – vazba na PACS;
- Specializovaný modul pro záznam operačních protokolů;
- Specializovaný modul pro endoskopické pracoviště;
- Specializovaný modul pro gynekologické a novorozenecké pracoviště;
- Anesteziologický protokol;
- Evidence pacientů v dispenzární péči;
- Generování pozvánek formou sms nebo e-mailu;
- Identifikace pacientů v rámci traumaplánu – hromadné neštěstí;
- Evidence dat Ošetřovatelské péče – Soběstačnost, Rány, pády dekubity;
- Nozokomiální nákazy;
- Omezovací prostředky;
- Nutriční skóre;
- Komunikace B2B (VZP);
- Identifikace uživatelů certifikátem;
- Přehledy a sestavy;
- Komunikace s externími programy (Svejkovský, Apotheka, , ICIP, VF-SED, KIS-DKC, ÚZIS, Gastromanažer, TEMPUS, NovaVoice, AMIS-H, e-nástěnka, PACS;
- Komunikace s externími subjekty (Datová rozhraní - SÚKL, ÚZIS, ČSSZ).

Do modulu Chorobopis jsou vkládána data následujícími způsoby:

- Data vkládaná pracovníky klinik a oddělení Zadavatele;
- Vstup a sdílení dat v modulu Přijímací kancelář;
- Sdílení dat obrazové dokumentace (PACS);
- Sdílení dat v modulech pracovišť komplementu;
- Sdílení dat v modulu Objednávky a žádanky.

Modul Chorobopis poskytuje data pro následující moduly nebo jiné informační systémy v rámci, a to:

- Data vstupující do modulu Přijímací kancelář;
- Data vstupující do modulu Objednávky a žádanky;
- Data vstupující do modulu Účty;
- Data vstupující do centrální databáze sdílených lékařských zpráv;

Centrální modul UNIS
Centrální modul UNIS zahrnuje následující funkcionality:

Přijímací kancelář

Modul Přijímací kancelář obsahuje následující výčet funkcionalit:
- Evidence hospitalizací pacientů – příjmů, překladů, propuštění;
- Evidence lůžkového fondu a obložnosti;
- Kontrolní systém vazby mezi záznamy o hospitalizaci a objednávkami stravy pro pacienty;
- Automatická vazba záznamů o hospitalizaci na účty pacientů a stravenky;
- Statistiky a přehledy podle zadaného období.

Data jsou do Modulu Přijímací kancelář zadávána následujícími způsoby:
- Data vkládaná pracovníky klinik a oddělení Zadavatele;
- Vstup dat z modulu Chorobopis.

Modul Přijímací kancelář poskytuje data pro:
- Sdílení dat v modulu Chorobopis.

Objednávání stravy pro pacienty

Modul Objednávání stravy pro pacienty obsahuje následující výčet funkcionalit:
- Evidence diet a individuálních výjimek ve stravě pacientů;
- Automatická vazba stravenek pacientů na záznamy hospitalizací;
- Objednávky stravy pacientů z oddělení;
- Objednávky mléčné stravy;
- Objednávky zásob na oddělení;
- Přebírání objednávek ze strany stravovacího provozu;
- Přehledy a sestavy.

Data jsou do modulu Objednávání stravy zadávána následujícími způsoby:
- Data vkládaná pracovníky klinik a oddělení Zadavatele z modulu Přijímací kancelář nebo z modulu Chorobopis.

Modul Objednávání stravy pro pacienty poskytuje data pro:
- Export formou textových souborů do systému stravovacího provozu dle stanoveného rozhraní.

Objednávky a žádanky

Modul Objednávky a žádanky obsahuje následující výčet funkcionalit:
- Elektronické žádanky pro vyšetření pacientů na pracovištích komplementu (laboratoře, RTG, transport, zvýšení úhrady, apod.).
- Data jsou do Modulu Objednávky a žádanky zadávána následujícími způsoby:
- Data zadávají pracovníci klinik a oddělení z modulu Přijímací kancelář nebo z modulu Chorobopis.

Modul Objednávky a žádanky pro pacienty poskytuje data pro:
- Informační systémy pracovišť komplementu.

Centrální historická databáze a registr + archiv

Modul Centrální historická databáze obsahuje následující výčet funkcionalit:
- Archivace a aktualizace osobních údajů pacientů;
- Archivace prvotních záznamů účtů;
- Archivace záznamů hospitalizací;
- Registrace pacientů v ordinaci závodního lékaře a stomatologů;
- Registr pojištěnců;
- Evidence dat Ošetřovatelské péče – Soběstačnost, Rány, pády dekubity;
- Nozokomiální nákazy;
- Omezovací prostředky;
- Identifikace pacientů v rámci traumaplánu – hromadné neštěstí;
- Centrové léky.

Data pro modul Centrální historická databáze jsou pořizována:
- Data z modulů Chorobopis, Přijímací kancelář, Účty;
- Data vkládaná pracovníky klinik a oddělení.

Modul Centrální historická databáze poskytuje data pro:
- Všechny moduly UNIS používajících osobní údaje pacientů;
- Každý pacient má jednoznačný a jedinečný identifikátor (centrální číslo pacienta), s kterým umí pracovat všechny moduly UNIS.

Účty za zdravotní péči

Modul Účty za zdravotní péči obsahuje následující výčet funkcionalit:
- Vedení účtů za lékařskou péči lůžkovou i ambulantní a zdravotnický transport včetně metodiky DRG;
- Modelace sestavení případu CZ DRG;
- Evidence plateb prostřednictvím pokladních lístků;
- Kontroly položek účtů (dle nastavení číselníků nebo fixních kontrol).

Data pro modul Účty za zdravotní péči jsou pořizována:
- Pracovníky klinik a oddělení Zadavatele přímo nebo prostřednictvím ostatních modulů UNIS.

Modul Účty za zdravotní péči poskytuje data pro:
- Moduly Účtárna a Statistika.

Číselníky a servisní nastavení

Modul Číselníky a servisní nastavení slouží pro správu veškerých číselníků systému UNIS daných legislativou či Zadavatelem. Dále obsahuje nastavení parametrů funkcí systému, formulářů a přístupových práv k systému UNIS.

Statistika

Modul Statistika obsahuje následující výčet funkcionalit:
- Přehled účtované zdravotní péče dle prvotních záznamů z pracovišť Zadavatele v souladu s platnými předpisy.

Data pro modul Statistika jsou pořizována:
- Automatizovaně z Účty za zdravotní péči.

Modul Statistika poskytuje data pro:
- Přehledy a sestavy.

Manager

Modul Manager využívá data z modulu Chorobopis za účelem
- dalšího zpracování na základě požadavků pracovišť.
- Zpracování statistik pro ÚZIS.

Editor dokladů

Modul Editor dokladů obsahuje následující výčet funkcionalit:
- Opravy účtů za zdravotní péči a transport na pracovištích;
- Výpis účtů za zdravotní péči a transport v konečné podobě;
- Systém indikátorů a časových razítek předání k opravě a předání opravených dokladů.

Do modulu Editor dokladů jsou pořizována data:
- Z modulu Účtárna;
- Pracovníky klinik a oddělení Zadavatele.

Modul Editor dokladů poskytuje data pro:
- Modul Účtárna;
- Přehledy a sestavy.

Účtárna výkonů

Modul Účtárna **výkonů** obsahuje následující výčet funkcionalit:
- Účty za zdravotní péči a transport (dle metodiky VZP) jako podklady pro účtování zdravotním pojišťovnám a jiným plátcům dle platných předpisů;
- Přehledy pro ÚZIS;
- Kontroly dokladů dle nastavení číselníků/kontrol;
- Sestavení případu CZ DRG.

Modul Účtárna **výkonů** pořizuje data:
- Z modulu Účty za zdravotní péči;
- Přímým zadáním Oddělením ZP.

Data z modulu Účtárna **výkonů** jsou poskytována pro:
- Dávky a protokoly pro zdravotní pojišťovny;
- Soubory pro hlášení na ÚZIS;
- Data vstupující do jiných provozovaných systémů.

Moduly pracovišť komplementu

Moduly pracovišť komplementu obsahují specifické funkcionality pro pracoviště komplementu v rámci FN Motol. Tyto funkcionality jsou z významné části unikátní na základě specifických potřeb a obsahují řadu integrací.

Systémy laboratoří a radiodiagnostického pracoviště

Systémy podporují činnost těchto oborů:
- laboratoř biochemie, hematologie, imunologie;
- laboratoř nukleární medicíny;
- laboratoř patologie;
- laboratoř mikrobiologie;
- laboratoř virologie;
- laboratoř likvorologie;
- krevní banka
- radiodiagnostické pracoviště.

Systémy laboratoří a radiodiagnostického pracoviště obsahují následující výčet funkcionalit:
- Příjem požadavků formou el. žádanek;
- Distribuce vzorků k analyzátorům;
- Napojení analyzátorů POCT na klinikách Zadavatele;
- Zpracování výsledků měření a vyšetření pacientů nebo biologického materiálu;
- Evidence kroků procesu (laboratoř patologie);
- Práce s textovou i obrazovou dokumentací;
- Kontroly výsledků;
- Export výsledků;
- Evidence chemikálií;
- Automatické účtování výkonů dle metodiky VZP;
- Přehledy a sestavy.

Data pro Systémy laboratoří a radiodiagnostického pracoviště jsou pořizována:
- Z modulu Objednávky a žádanky (elektronické žádanky);
- Pracovníky laboratoří podle žádanek o vyšetření z ostatních pracovišť;
- Z analyzátorů a dalších přístrojů;
- Výsledky měření a popis vyšetření.

Systémy laboratoří a radiodiagnostického pracoviště poskytují data pro:
- Sdílení dat v modulech pracovišť komplementu;
- Sdílení dat v modulu Chorobopis;
- Data vstupující do modulu Účty za zdravotní péči;
- Export dat do systému ICIP - textové soubory dle DaSta;
- Export zakódovaných výsledků pro vnější objednatele dle DaSta;
- Export výsledků a vyžádaných dat do systémů ÚZIS (např. ISIN) – XML dle DaSta.

Nahlížení do výsledků vyšetření pracovišť Komplementu

Modul Nahlížení do výsledků vyšetření pracovišť Komplementu obsahuje prohlížení výsledků měření a vyšetření provedených na pracovištích komplementu.

Data do modulu Nahlížení do výsledků vyšetření pracovišť Komplementu jsou pořizována pracovníky Komplementu nebo vstupují automatizovaně na základě integrace s laboratorní technikou nebo jinými přístroji.

Výstup z modulu Nahlížení do výsledků vyšetření pracovišť Komplementu je:
- Přehled výsledků měření a popis vyšetření na pracovištích komplementu u jednotlivých pacientů.

Transfuzní oddělení (UNIS Amadeus - moduly Dárce, Výrobna, Sklad)

Modul **Dárce** obsahuje následující výčet funkcionalit:
- Evidence dárců a odběrů;
- Laboratorní testy spojené s odběrem a odběr;
- Řízení výroby a uskladnění transfuzních přípravků;
- Přehledy a sestavy.

Data pro modul Dárce jsou:
- Vkládaná pracovníky transfuzního oddělení;
- Výsledky měření a vyšetření, klinická data.

Modul Dárce oddělení poskytuje data pro:
- modul Účty za zdravotní péči.

Modul **Výrobna** obsahuje následující výčet funkcionalit:
- Odběr - lékařská kontrola;
- Zápis a štítkování výrobků;
- Řízení výroby a uskladnění transfuzních přípravků;
- Přehledy a sestavy.

Data pro modul Výrobna jsou:
- Vkládaná pracovníky transfuzního oddělení;
- Výsledky měření a vyšetření, klinická data.

Modul Výrobna poskytuje data pro:
Modul **Sklad** ----------
Modul **Sklad** obsahuje následující výčet funkcionalit:
- Evidence (skladové hospodářství) transfuzních přípravků;
- Skladové hospodářství diagnostik;
- Laboratorní imunohematologická vyšetření;
- On-line napojení analyzátorů obousměrně;
- On-line napojení ozařovače krve;
- Přehledy a sestavy.

Data pro modul Sklad jsou:
- Vkládaná pracovníky transfuzního oddělení;
- Výsledky měření a vyšetření, klinická data.

Modul Sklad poskytuje data pro:
- modul Účty za zdravotní péči;
- sdílení dat s modulem Chorobopis a komplement

Modul Faktura

Modul Faktura slouží k vytváření podkladů pro fakturaci zdravotní péče o cizince

Modul Faktura obsahuje následující výčet funkcionalit:
- Evidence samoplátců;
- Kalkulace ceny faktury dle plátce;
- Evidence pohledávek;
- Tržby- zjednodušený daňový doklad;
- Tisk speciálních dokumentů (např. smlouvy).

Data pro modul Faktura jsou pořizována pracovníky Oddělení péče o samoplátce

Modul Faktura poskytuje data pro systém AMIS.

Žádanky (fasování sklad MTZ, řemeslnické práce, zdr. materiál, léky aj.)

Modul Žádanky slouží k objednávání služby či materiálu (požadavku) v rámci organizace formou elektronické žádanky. Požadavky jsou vkládány na klinikách/odděleních do programu Žádanky ve tvaru el. formuláře a odesílány na centrální dispečink či přímo profesím k realizaci.

Modul Žádanky obsahuje následující výčet funkcionalit:
- Tvorba žádanky – zadání položkové žádanky a textové žádanky, oprava, storno, odeslání, šablona, kopie, tisk žádanky;
- Schvalování žádanek – víceúrovňové schvalování žádanek – vedoucím oddělení a vedoucím úseku, vrácení žádanky o 1 stupeň zpět či zadavateli;

- Zpracování žádanky centrálním dispečinkem – předání žádanky na příslušný dispečink správy;
- Zpracování žádanky dispečerem správy – přidělení žádanky příslušné profesi k realizaci a tisk pracovního listu;
- Realizace žádanky – tisk požadavku (žádanky) resp. pracovního listu, zápis provedených prací a spotřebovaného materiálu, odpracovaných hodin, realizátora;
- Uživatelská oprávnění – oprávnění jednotlivým uživatelům na typ žádanky a nákladové středisko, oprávnění na schvalování, zpracování a realizaci žádanek.

Data ze Žádanek jsou poskytována pro:

- Apotheka – žádanky na léky a zdravotnický materiál prostřednictvím SYNC

Data pro Žádanky jsou pořizována:

- pracovníky klinik a oddělení Zadavatele;
- z dat Apotheka – číselníky léků a zdravotnického materiálu prostřednictvím SYNC;
- z dat centrálních číselníků zaměstnanců, nákladových středisek a stanic TabCent.

Všechny součásti UNIS musí být udržovány v souladu s aktuálně platnou legislativou a ostatními souvisejícími předpisy v rámci výkonu zdravotní péče v FNM a to zejména výkaznictví vůči zdravotním pojišťovnám a dalším povinným subjektům.

Příloha č. 3 Smlouvy

Ceník Služeb

Průběžně poskytované Služby

Položka	MJ	Cena za 1 MJ (Kč bez DPH)
Průběžně poskytované Služby Modul Chorobopis	1 měsíc	694 000,-
Průběžně poskytované Služby Centrální modul UNIS (zahrnuje funkcionality: Přijímací kancelář, Objednávání stravy pro pacienty, Objednávky a žádanky, centrální historická databáze + registr + archiv	1 měsíc	40 000,-
Průběžně poskytované Služby Modul Účtárna (zahrnuje funkcionality Účty za zdravotní péči, Číselníky a servisní nastavení, Statistika, Manager, Editor dokladů, Účtárna výkonů	1 měsíc	107 000,-
Průběžně poskytované Služby Modul Transfuzní oddělení (Dárce, Výrobna, Sklad)	1 měsíc	26 000,-
Průběžně poskytované Služby Modul Faktura	1 měsíc	5 000,-
Průběžně poskytované Služby Modul Žádanky (fasování sklad MTZ, řemeslnické práce, zdr. materiál, léky aj.)	1 měsíc	15 000,-
Průběžně poskytované Služby Modul Pracoviště komplementu (zahrnuje laboratoř: biochemie, hematologie, imunologie, mikrobiologie, patologie, nukleární medicíny, likvorologie, krevní banka, radiodiagnostické pracoviště, nahlížení do výsledků vyšetření)	1 měsíc	480 000,-

Služby na objednávku

Položka	MJ	Cena za 1 MJ (Kč bez DPH)
Rozvoj Systému	1 člověkoden	8 000,-
Školení k Systému	1 člověkoden	8 000,-
Napojení analyzátoru	1 člověkoden	8 000,-
Další služby	1 člověkoden	8 000,-

Příloha č. 4 Smlouvy

Poddodavatelé

Nebude plněno poddodavatelsky.

Příloha č. 5 Smlouvy

Metodika řízení dodavatelů

Metodika řízení dodavatelů definuje pravidla, postupy a náležitosti v průběhu celého životního cyklu dodávky, tedy od výběru dodavatele, přes průběh realizace plnění, po splnění smluvního závazku, ukončení smlouvy a závěrečné hodnocení zkušeností s dodavatelem.

Proces řízení dodavatelů musí být v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů a zákonem č. 134/2016 Sb., o zadávání veřejných zakázek (zákon o zadávání veřejných zakázek), ve znění pozdějších předpisů.

Rozsah platnosti

Metodika řízení dodavatelů se vztahuje na všechny informace, které jsou uloženy, spravovány nebo používány v informačních systémech, bez ohledu na formu, formát, nosné médium, nebo zda se jedná o zpracování automatizované nebo ruční.

Metodika řízení dodavatelů se dále vztahuje na všechny zdroje používané pro tvorbu, zpracování, přenos, ukládání, užívání a kontrolu těchto informací.

Definice a použité zkratky

Architekt kybernetické bezpečnosti navrhuje základní bezpečnostní architekturu informačních a komunikačních systémů, jejich jednotlivých komponent, vzájemných vazeb a dohlíží na soulad implementace architektury informačních a komunikačních systémů se systémem řízení kybernetické bezpečnosti.

Dodavatel je každý, kdo poskytuje dodávky, služby nebo stavební práce a vstupuje do právního vztahu s povinnou osobou. Dodavatelem je provozovatel informačního nebo komunikačního systému, významný dodavatel a každý dodavatel, který nesplní definici provozovatele informačního nebo komunikačního systému či významného dodavatele.

Garant aktiva je fyzická osoba pověřená k zajištění rozvoje, použití a bezpečnosti aktiva. Garant aktiva je vlastníkem aktiva nikoliv z pohledu majetkového, ale odpovědnostního, je odpovědný za chod aktiva po obsahové stránce, definuje požadavky na zabezpečení aktiva z pohledu důvěrnosti, dostupnosti a integrity dat.

Manažer kybernetické bezpečnosti je pracovník, který odpovídá za systém řízení kybernetické bezpečnosti.

Provozovatel informačního nebo komunikačního systému – § 2 písm. g) ZKB je „orgán nebo osoba zajišťující funkčnost technických a programových prostředků tvořících informační nebo komunikační systém“. Provozovatel je vždy významným dodavatelem.

Služby jsou funkce, které uživatelům umožňují přístup a práci s daty (pořizování, ukládání / uchování - včetně tvorby kopií, přenos, transformace / modifikace (změny formátu, šifrování, mazání), prezentace (digitální publikování na webových stránkách, promítání) nebo jejich tisk.

Výbor pro řízení kybernetické bezpečnosti je nejvyšší orgán pro oblast kybernetické bezpečnosti, který řídí a kontroluje dodržování pravidel kybernetické bezpečnosti.

Významný dodavatel – § 2 písm. g) VKB je „provozovatel informačního nebo komunikačního systému a každý, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti informačního a komunikačního systému“.

Zadavatel je osoba, která k úhradě nadlimitní nebo podlimitní veřejné zakázky použije více než 200 000 000 Kč, nebo více než 50 % peněžních prostředků, poskytnutých z:

a) rozpočtu veřejného zadavatele,

b) rozpočtu Evropské unie nebo veřejného rozpočtu cizího státu s výjimkou případů, kdy je veřejná zakázka plněna mimo území Evropské unie.“

Zaměstnanec odpovědný za smluvní vztah je zaměstnanec, který určuje a řídí všechny odborné záležitosti související s předmětnými dodávkami nebo službami, měl by disponovat odborným povědomím o věcném plnění.

NÚKIB Národní úřad pro kybernetickou a informační bezpečnost.

SLA Smlouva o úrovni poskytovaných služeb, která definuje rozsah, úroveň a intenzitu služeb při podpoře informačních a komunikačních technologií (Service Level Agreement).

VKB Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů.

ZKB Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.

ZZVZ Zákon č. 134/2016 Sb., o zadávání veřejných zakázek (zákon o zadávání veřejných zakázek), ve znění pozdějších předpisů.

Proces řízení dodavatelů

Řízení dodavatelů je jedním z organizačních bezpečnostních opatření, k jejichž provádění jsou povinny osoby spadající do působnosti ZKB.

Tyto osoby jsou současně povinny zohlednit požadavky vyplývající ze všech bezpečnostních opatření podle ZKB při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou.

V rámci řízení všech svých dodavatelů je povinná osoba povinna:

- stanovit pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací,
- seznamovat své dodavatele s těmito pravidly a vyžadovat jejich plnění,
- řídit rizika spojená s dodavateli,
- zajistit poučení dodavatelů o jejich povinnostech a o bezpečnostní politice v rámci řízení bezpečnosti lidských zdrojů,
- zajistit oznamování neobvyklého chování systému a podezření na jakékoliv zranitelnosti v rámci zvládání kybernetických bezpečnostních incidentů.

Dále je povinná osoba povinna:

- vést evidenci svých významných dodavatelů a o vedení v evidenci významné dodavatele prokazatelně písemně informovat,
- u významných dodavatelů v rámci výběrových řízení a před uzavřením smlouvy provádět hodnocení rizik souvisejících s plněním předmětu výběrového řízení,
- v rámci uzavíraných smluvních vztahů stanovit způsoby a úrovně realizace bezpečnostních opatření a určit obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření,
- provádět pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných plnění pomocí vlastních zdrojů nebo pomocí třetí strany a v reakci na rizika a zjištěné nedostatky zajistit jejich řešení,
- zajistit, aby smlouvy, které jsou s významnými dodavateli uzavírány, obsahovaly relevantní oblasti uvedené v příloze č. 7 k VKB [§ 8 odst. 1 písm. f) VKB]
- pravidelně přezkoumávat plnění smluv s významnými dodavateli.

Nastavení procesu

Nstavení procesu řízení dodavatelů souvisí s definicí postupu v jednotlivých etapách životního cyklu řízení služeb:

a) Během definování předmětu plnění budoucí smlouvy je nezbytné provést hodnocení rizik souvisejících s předmětem plnění, jedná-li se o smlouvu na provoz, rozvoj nebo akvizici informačního systému, nákup hardware, software či služeb. Hodnocení rizik souvisejících s předmětem plnění je nezbytné zohlednit již v zadávací dokumentaci a následně ve smlouvě s dodavatelem.

b) Po definování předmětu plnění lze na základě veřejně dostupných zdrojů či průzkumu trhu odhadnout potenciální okruh dodavatelů a v daný okamžik realizovat hodnocení rizik souvisejících s potenciálními dodavateli a zohlednit výsledky hodnocení ve smlouvě či zadávací dokumentaci.

c) Je-li předmětem smlouvy na provoz či rozvoj informačního systému, je nezbytné po uzavření smlouvy provést hodnocení rizik souvisejících s akvizicí nového informačního systému a jeho provozem, které se realizuje společně s dodavatelem. Pokud bude vyhodnoceno riziko, musí být stanoven způsob opatření k jeho ošetření nebo zmírnění a harmonogram vypořádaní.

d) V průběhu plnění smlouvy musí být prováděno pravidelné hodnocení rizik ať již z důvodu zohledňování nově vydaných opatření NÚKIB, významných změn v provozním prostředí, organizačních nebo obchodních změnách prostředí dodavatele služeb nebo produktů, nebo jako pravidelné vyhodnocení stavu plnění smlouvy.

e) Po ukončení smluvního vztahu musí dojít ke konečnému vyhodnocení dodavatele, které může být využito pro další smluvní vztahy a veřejné zakázky.

Typy dodavatelů

VKB rozlišuje tři základní typy dodavatelů:

- běžní dodavatelé,
- významní dodavatelé,
- provozovatelé (podmnožina významných dodavatelů).

Povinnosti související se všemi dodavateli

U všech svých dodavatelů je povinná osoba povinna:

- stanovit pravidla pro dodavatele zohledňující požadavky systému řízení bezpečnosti informací [§ 8 odst. 1 písm. a) VKB],
- zpřístupnit dodavatelům v listinné nebo elektronické podobě relevantní bezpečnostní dokumentaci [§ 8 odst. 1 písm. d) VKB],
- kontinuálně řídit rizika spojená s dodavateli [§ 8 odst. 1 písm. e) VKB],
- stanovit způsob poučení dodavatele o jeho povinnostech a o bezpečnostní politice [§ 9 odst. 1 písm. a) bod 1. VKB],
- stanovit způsob a formu vstupních a pravidelných školení pro dodavatele v souladu s plánem rozvoje bezpečnostního povědomí [§ 9 odst. 1 písm. c) VKB],
- stanovit, jakým způsobem budou dodavatelé oznamovat neobvyklé chování informačního a komunikačního systému a podezření na jakékoliv zranitelnosti [§ 14 odst. 1 písm. f) VKB].

Povinnosti související s významným dodavatelem

Ve vztahu ke svým významných dodavatelů je povinná osoba povinna:

- řídit se všemi povinnostmi souvisejícími s dodavateli podle podkapitoly 2.1,
- zařadit významného dodavatele do evidence významných dodavatelů [§ 8 odst. 1 písm. b) VKB] (vzor Příloha č. 2), která obsahuje seznam všech významných dodavatelů, základní informace o smluvních vztazích s významnými dodavateli, a informace o přístupnosti jednotlivých formulářů hodnocení významných dodavatelů,

- prokazatelně písemně informovat významného dodavatele o jeho evidenci jako významného dodavatele [§ 8 odst. 1 písm. c) VKB], prokazatelné písemné informování významného dodavatele je možné provést již ve smlouvě, nebo samostatným dokumentem, a musí obsahovat identifikaci správce nebo provozovatele, identifikaci informačního nebo komunikačního systému, identifikaci významného dodavatele a obsah pravidel zohledňujících požadavky systému řízení bezpečnosti informací [§ 8 odst. 3 VKB],
- zajistit soulad smluv uzavíraných s významnými dodavateli s požadavky uvedenými v příloze č. 7 VKB [§ 8 odst. 1 písm. f) VKB],
- pravidelně přezkoumávat plnění smluv uzavřených s významnými dodavateli, a to včetně zavedených bezpečnostních opatření u poskytnutého plnění [§ 8 odst. 1 písm. g) VKB],
- provést v rámci výběrového řízení, příp. před uzavřením smlouvy hodnocení rizik souvisejících s plněním předmětu výběrového řízení [§ 8 odst. 2 písm. a) VKB],
- stanovit v uzavíraných smlouvách způsob a úrovně realizace bezpečnostních opatření a určit obsah vzájemné odpovědnosti za zavádění a kontrolu bezpečnostních opatření [§ 8 odst. 2 písm. b) VKB],
- provádět pravidelné hodnocení rizik [§ 8 odst. 2 písm. c) VKB],
- v reakci na rizika a zjištěné nedostatky zajistit jejich řešení [§ 8 odst. 2 písm. d) VKB].

Povinnosti související s provozovatelem informačního nebo komunikačního systému

Povinnosti správce

Ve vztahu k provozovateli informačního nebo komunikačního systému je správce tohoto systému povinen:

- řídit se všemi povinnostmi souvisejícími s dodavateli a významnými dodavateli
- zařadit provozovatele do evidence významných dodavatelů [§ 8 odst. 1 písm. b) VKB]
- prokazatelně písemně informovat provozovatele o jeho evidenci jako provozovatele [§ 8 odst. 1 písm. c) VKB], prokazatelné písemné informování provozovatele je možné provést již ve smlouvě, nebo samostatným dokumentem, a musí obsahovat identifikaci správce nebo provozovatele, identifikaci informačního nebo komunikačního systému, identifikaci významného dodavatele a obsah pravidel zohledňujících požadavky systému řízení bezpečnosti informací [§ 8 odst. 3 VKB],
- dohodnout se na rozsahu plnění požadavků ZKB a VKB.

Povinnosti provozovatele

Identifikovaný a informovaný provozovatel je povinen plnit povinnosti podle ZKB a VKB. V rámci plnění se bude jednat především o povinnosti:

- hlásit kontaktní údaje NÚKIB [§ 8 odst. 4 VKB],
- zavádět bezpečnostní opatření [§ 4 odst. 2 ZKB],
- hlásit kybernetické bezpečnostní incidenty [§ 8 odst. 1 ZKB],
- provádět opatření podle § 11 ZKB.

Mezi další povinnosti patří povinnost předávat správci data, provozní údaje a informace na jeho vyžádání [§ 6a odst. 2 ZKB], při ukončení spolupráce [§ 6a odst. 3 ZKB] a na základě rozhodnutí vydaného NÚKIB [§ 15a ZKB].

Dále má provozovatel povinnost provádět audit kybernetické bezpečnosti a jeho výsledky předkládat správci [§ 16 VKB].

S identifikovaným a informovaným provozovatelem je nutné si dohodnout rozsah zavádění a provádění bezpečnostních opatření, a to tak, jak je to nezbytné pro zajištění kybernetické bezpečnosti informačního nebo komunikačního systému. V podrobnostech se problematice povinností provozovatelů informačních a komunikačních systémů věnuje podpůrný materiál NÚKIB k provozovateli informačního nebo komunikačního systému.

Stanovení pravidel bezpečnosti pro dodavatele zohledňující požadavky systému řízení bezpečnosti informací

Pravidla bezpečnosti pro dodavatele musí být stanovena ve formě dokumentace upravené speciálně pro dodavatele, která obsahuje všechny relevantní informace.

Způsob a forma seznámení dodavatele s pravidly

V režimu ZZVZ zadavatel (objednatel) jako součást zadávací dokumentace veřejné zakázky předloží potenciálním dodavatelům obchodní a platební podmínky plnění veřejné zakázky (např. ve formě závazného textu návrhu smlouvy nebo jiného samostatného dokumentu), jehož znění dodavatelé nebudou oprávněni měnit ani doplňovat (s výjimkou výslovně označených míst).

Součástí zadávací dokumentace musí být informování o významnosti dodavatele, tedy zda bude dodavatel provozovatelem, významným dodavatelem nebo dodavatelem (aby měli dodavatelé kompletní informace o předmětu plnění a rozsahu jejich povinností plynoucích jak ze smlouvy, tak ze ZKB).

Mimo režim ZZVZ objednatel specifikuje požadavky na předmět plnění, včetně vyhláškou požadovaných ustanovení, zapracuje je do návrhu smlouvy (nebo do jiného samostatného dokumentu) a ten následně předloží dodavateli.

Životní cyklus dodavatelského vztahu

Hodnocení dodavatelů a rizik s nimi spojených musí probíhat v průběhu celého životního cyklu dodavatelského vztahu, tzn. ve fázi formulace požadavků na předmět smlouvy, výběru dodavatele, ve fázi plnění smluvního vztahu a po jeho skončení.

Pravidla a principy pro výběr dodavatelů

V rámci výběru dodavatelů poptávaného plnění jsou zohledňovány identifikované bezpečnostní potřeby v souladu s interními a právními předpisy.

Pravidla pro výběr dodavatele musí zohledňovat základní bezpečnostní požadavky, resp. způsob jejich určení, hodnocení rizik souvisejících s dodavatelem a stanovenou úroveň zabezpečení.

Významnými faktory pro určení konkrétní úrovně požadavků na dodavatele musí být především:

- charakter informačního nebo komunikačního systému, do nějž bude dodavatel svým plněním zasahovat (informační systém základní služby,
- charakter dodavatele, tedy zda jde o „běžného“ dodavatele, významného dodavatele nebo provozovatele systému, příp. specifika vztahu dodavatele k systému, do kterého bude svým plněním zasahovat.

Při tvorbě pravidel musí být zohledněny i relevantní vnitřní předpisy organizace nebo závazné pokyny nadřízených subjektů.

Výběr dodavatelů musí být založen na výsledcích hodnocení rizik spojených s předmětem výběrového řízení a rizik souvisejících s významnými dodavateli [tzv. předsmluvní hodnocení rizik podle § 8 odst. 2 písm. a) VKB].

Zadavatel při postupu podle ZZVZ nesmí vznést jiné kvalifikační požadavky na osobu dodavatele (příp. poddodavatele) než které mu ZZVZ výslovně umožňuje. Zbylé požadavky je třeba přetransformovat na požadavky na předmět plnění, a nevázat je na osobu dodavatele.

Identifikované bezpečnostní potřeby jsou formou jednotlivých požadavků zahrnuty do smluv, resp. do zadávacích podmínek, pokud je dodavatel vybírán v režimu ZZVZ (míra podrobnosti iniciačních zadávacích podmínek bude závislá na zvoleném druhu zadávacího řízení).

V rámci spolupráce s dodavatelem musí být určen odpovědný zaměstnanec pro každého jednotlivého dodavatele, tzv. zaměstnanec odpovědný za smluvní vztah. Tento zaměstnanec musí určit a řídit všechny odborné záležitosti související s předmětnými dodávkami nebo službami, měl by tedy disponovat odborným povědomím o věcném plnění a zároveň i případnou právní podporou. Nedílnou součástí těchto aktivit je i zajištění úrovně bezpečnosti informací.

Pravidla pro hodnocení rizik souvisejících s dodavateli

Hodnocení rizik souvisejících s dodavateli je součástí specifikace předmětu plnění a přípravy zadávací dokumentace v režimu ZZVZ. Toto hodnocení rizik musí být zpracováno jednotnou metodikou.

Za provedení hodnocení rizik souvisejících s dodavateli odpovídá obvykle zaměstnanec odpovědný za smluvní vztah v součinnosti s garantem primárního aktiva a garantem podpůrného

aktiva. Pokud se na hodnocení rizik nepodílí přímo i manažer kybernetické bezpečnosti, musí být o něm informován.

Pravidla pro hodnocení rizik souvisejících s předmětem plnění

Riziky souvisejícími s plněním předmětu výběrového řízení ve smyslu § 8 odst. 2 písm. a) VKB jsou nejen rizika spojená se samotným předmětem plnění, nýbrž i rizika spojená s dodavatelem poptávaného plnění. Povinnost provádět toto tzv. předsmluvní hodnocení rizik se uplatní ve vztahu k významným dodavatelům (provozovatelům), nicméně je samozřejmě možné aplikovat tento postup i ve vztahu ke všem ostatním dodavatelům (pokud to odůvodňují potřeby povinné osoby).

U každého poptávaného plnění musí být určena jeho významnost, tedy zda bude jeho dodavatel označen jako provozovatel, významný dodavatel nebo běžný dodavatel. Toto určení by měla provést osoba odpovědná za konkrétní smluvní vztah.

Pravidla pro hodnocení rizik souvisejících s předmětem plnění (tj. i s dodavateli poptávaného plnění) by měla korespondovat se standardními postupy pro hodnocení rizik spojených s již implementovaným plněním. Lze akceptovat i situaci, kdy jsou pravidla pro tzv. předsmluvní hodnocení rizik uzpůsobena specifikům dané situace, kdy povinná osoba mnohdy nemusí disponovat kompletními informacemi o předmětu plnění nebo o jeho dodavateli (zvláště v situacích, kdy je dodavatel vybírán v zadávacím řízení, u něhož je třeba stanovit zadávací podmínky předem a v němž již není možné reagovat na vývoj situace, tedy zejm. v otevřeném a užším řízení). V každém případě je třeba, aby byla pravidla nastavena předem, transparentně, smysluplně a pokud možno univerzálně, tedy aby nebyla neodůvodněně přizpůsobována jednotlivým výběrovým řízením.

Dále je potřeba, aby pravidla pro hodnocení rizik souvisejících s předmětem plnění (a dodavateli) odpovídala požadavkům VKB, tedy aby bylo hodnocení rizik prováděno přiměřeně podle přílohy č. 2 k VKB.

V rámci hodnocení rizik je možné využít přílohu č. 3 k VKB, která obsahuje vybrané kategorie hrozeb a zranitelností. Výsledný a konkrétní organizaci uzpůsobený katalog hrozeb a zranitelností (potažmo kompletních rizik) má představovat znalostní bázi, která je na základě zkušeností pravidelně doplňována a slouží jako pomůcka pro osobu zodpovědnou za hodnocení rizik. Za údržbu katalogu hrozeb, zranitelností a rizik je zpravidla odpovědný manažer kybernetické bezpečnosti, na obsahu se podílejí všechny osoby, které musí provádět hodnocení rizik související s řízením dodavatelů. Výsledný katalog rizik by měl obsahovat konkrétní rizika využitelná v organizaci povinné osoby, stejně jako rizika specifická právě pro oblast, v níž organizace působí.

Postup hodnocení rizik před uzavřením smlouvy u významných dodavatelů

Ustanovení § 8 odst. 2 písm. a) VKB požaduje, aby bylo v rámci výběrového řízení a před uzavřením smlouvy provedeno hodnocení rizik souvisejících s plněním předmětu výběrového řízení. Konkrétní postup je tedy třeba přizpůsobit specifickým skutkovým okolnostem. Pokud jde o osobu nespadající do působnosti ZZVZ, je možné hodnocení rizik provést skutečně až před podpisem smlouvy (pokud to konkrétní okolnosti uzavírání smluvního vztahu nevylučují). Pokud jde o osobu spadající
do působnosti ZZVZ (a ta nepostupuje na základě některé ze zákonných výjimek), je potřeba konkrétní postup přizpůsobit druhu zadávacího řízení, který byl pro výběr dodavatele zvolen. U transparentních druhů zadávacího řízení musí být provedeno kompletní předsmluvní hodnocení rizik již ve fázi tvorby zadávacích podmínek (neboť ty již nemohou být po uplynutí lhůty pro podání nabídek měněny), u méně transparentních druhů řízení (např. jednacího řízení) je možné provést hodnocení rizik až v pozdějších fázích zadávacího řízení.

Před uzavřením smlouvy musí být provedeno hodnocení rizik s ohledem na konkrétní předmět plnění smlouvy. Hodnocení rizik je prováděno podle k tomu určené metodiky pro identifikaci a hodnocení aktiv a rizik, vytvořené podle § 4 VKB a § 5 VKB, s ohledem na důležitost dodávky.

V případě, že není k dispozici dostatek informací o předmětu veřejné zakázky nebo o jejích potenciálních dodavatelích, musí být hodnocení rizik provedeno alespoň na obecné úrovni. Výstupem může být identifikace potenciálně rizikových míst, na která je potřeba se zaměřit, aby nevznikl problém. V rámci hodnocení rizik spojených s dodavateli je možné využít jednak informace univerzálně platné pro jakékoli dodavatele, jednak informace vztahující se ke konkrétním dodavatelům. Informace o potenciálních dodavatelích poptávaného plnění je možné získat zejm. v rámci průzkumu trhu realizovaného před zahájením výběrového řízení (případně v průběhu výběrového řízení, pokud to situace umožňuje, v případě řízení podle ZZVZ půjde zejm. o jednací řízení, příp. zadání veřejné zakázky mimo zadávací řízení). Otevřenost výběrového řízení a šíře okruhu potenciálních dodavatelů povinnou osobu nezbavuje povinnosti hodnotit rizika spojená s potenciálními dodavateli ještě před uzavřením smlouvy.

Při hodnocení rizik jsou hodnocena inherentní rizika, resp. v případě již zavedených bezpečnostních opatření i tato opatření, a následně jsou zohledněna bezpečnostní opatření, která vyplývají z bezpečnostních pravidel pro dodavatele, zohledněna relevantní ustanovení uvedená v příloze č. 7 k VKB a doplněna bezpečnostní opatření, která se vztahují ke konkrétnímu plnění, tak, aby výsledné hodnoty identifikovaných rizik byly z pohledu zavedených politik akceptovatelné. Zvolená bezpečnostní opatření musí být zohledněna v uzavírané smlouvě.

V závislosti na způsobu výběru dodavatele je pak třeba zvolená bezpečnostní opatření buďto zahrnout již do podmínek výběrového řízení, nebo je zohlednit či upravit až v průběhu řízení (při zohlednění dalších informací, které povinná osoba v průběhu jednání s dodavateli získala).

V takovém případě dojde následně po výběru dodavatele k porovnání hodnocení dodavatele v jednotlivých oblastech s hodnocením rizik dodávaného plnění. Na základě výsledku tohoto porovnání mohou být přijata dodatečná bezpečnostní opatření, která musí být zohledněna ve smlouvě.

Za hodnocení rizik a výběr relevantních bezpečnostních opatření zpravidla odpovídá zaměstnanec odpovědný za smluvní vztah a architekt kybernetické bezpečnosti. V případě, že organizace nemá obsazenou roli architekta kybernetické bezpečnosti, mělo by se jednat o zaměstnance, který má v náplni práce navrhování a implementaci bezpečnostních opatření.

Minimální skutečnosti posuzované při hodnocení rizik souvisejících s předmětem plnění

Při posuzování hodnocení rizik je nutné zohlednit minimálně následující oblasti:

- rozsah prostředků a informací, ke kterým bude umožněn přístup,
- hodnota, citlivost a kritičnost primárních aktiv, ke kterým bude umožněn přístup,
- typ požadovaného přístupu:
- fyzický – budovy, kanceláře, místnosti s počítači, spisovny,
- logický – data, informační systémy, aplikace,
- rozsah přidělených privilegovaných oprávnění,
- realizovaná opatření bezpečnosti informací a jejich stav,
- formy výběru a určení osob, které se budou podílet na plnění závazků, a způsoby jejich seznámení s bezpečnostními politikami a pravidly,
- postupy pro řešení bezpečnostních incidentů,
- zákonné, smluvní a jiné požadavky, které ovlivňují vztah s dodavatelem,
- použití poddodavatele dodavatelem pro zajištění dodávky služby,
- vliv rizik na zájmy povinné osoby,
- riziko související s upozorněními vládního CERT, varováními, ochrannými a reaktivními opatřeními či jinými instrumenty využívanými NÚKIB pro zvýšení bezpečnosti informací,
- další relevantní rizika související s předmětem výběrového řízení.

Postup podle ZZVZ

Při výběru dodavatele v otevřeném řízení podle ZZVZ je možné postupovat dvěma způsoby:

a) hodnotit rizika spojená s předmětem plnění (a tedy i s jeho potenciálními dodavateli) před zahájením samotného řízení, ve fázi tvorby zadávacích podmínek, a zvolená bezpečnostní opatření zahrnout do zadávacích podmínek (a případného návrhu smlouvy), nebo

b) hodnotit rizika spojená s předmětem plnění (a tedy i s jeho potenciálními dodavateli) ve fázi hodnocení nabídek.

Konkrétní podoba předsmluvního hodnocení rizik je odpovědností povinné osoby. Pokud bude toto hodnocení provedeno příliš obecně, bez vynaložení přiměřeného úsilí pro získání dostatku relevantních informací o rizicích souvisejících s předmětem plnění a potenciálními dodavateli, výsledkem bude uzavření smlouvy neodpovídající požadavkům ZKB a VKB. Uvedení smlouvy do souladu s požadavky ZKB bude následně odpovědností povinné osoby.

Postup pravidelného hodnocení rizik souvisejících s předmětem plnění během smluvního vztahu

Po uzavření smluvního vztahu, resp. po implementaci dodaného plnění, je hodnocení rizik dodávky zapracováno do standardního procesu hodnocení aktiv a rizik, který musí zohledňovat mj. případné vydání varování, reaktivních a ochranných opatření a výsledky kontrol zavedených bezpečnostních opatření. Tento proces probíhá podle interní metodiky organizace. Dodávka je včleněna
do informačního nebo komunikačního systému, u kterého standardně probíhá hodnocení aktiv a rizik podle § 4 a § 5 VKB.

Za promítnutí rizik spojených s dodávkou do standardního hodnocení aktiv a rizik v rámci organizace odpovídá obvykle manažer kybernetické bezpečnosti.

Výsledek hodnocení rizik souvisejících s předmětem plnění

Výsledky hodnocení rizik souvisejících s předmětem plnění a dodavateli jsou součástí specifikace plnění, příp. zadávací dokumentace, kde jsou uvedena příslušná bezpečnostní opatření, a to ještě před uzavřením smlouvy.

Výsledky hodnocení rizik dodavatelů a příslušná opatření u již uzavřených smluvních vztahů a které ovlivní primární nebo podpůrná aktiva nesmí být v rozporu s uzavřenou smlouvou a příp. veřejnou zakázkou, na jejímž základě byla tato smlouva uzavřena. Pokud jsou identifikovány rozpory, přichází v úvahu:

a) prověřit, zda jsou všechny smluvní strany ochotné uzavřít příslušný dodatek smlouvy,

b) znovu projednat smluvní vztah v režimu změn podle § 222 ZZVZ, neboť se jedná o změnu smlouvy, jejíž potřeba vznikla v důsledku okolností, které zadavatel jednající s náležitou péčí nemohl předvídat, ve smyslu § 222 odst. 6 písm. a) ZZVZ; nemožnost předvídat takovou změnu je dána nemožností předvídat vývoj v oblasti legislativního procesu,

c) pokud nebude nalezena shoda na uzavření dodatku smlouvy, prostřednictvím čerpání kapacit dodavatele zajistit všechny povinnosti dodavatele, u nichž je to možné (např. povinnost poskytovat zadavateli součinnost při plnění jeho povinností podle ZKB a jeho prováděcích předpisů, povinnost vypracovat a předložit havarijní plány apod.); pokud tato možnost není v uzavřené smlouvě dána nebo je již vyčerpána jinými potřebami, zohlednit všechny chybějící povinnosti v hodnocení rizik.

Ukončení smluvního vztahu u významných dodavatelů

Při ukončení smluvního vztahu významného dodavatele se zpravidla jedná o významnou změnu a následuje odpovídající postup, který zahrnuje také aktualizaci hodnocení rizik.

Postup v případě, že nastane významná změna, popisuje interní dokument organizace podle § 11 VKB a její přílohy č. 5: 1.21. Politika řízení změn.

Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti

Předně, obsahem smlouvy (příp. jiného závazného dokumentu smluvních stran) musí být informace o tom, že smlouva se týká informačního nebo komunikačního systému spadajícího do působnosti ZKB. Současně je vhodné, aby již v těle smlouvy byla obsažena informace o tom, zda je dodavatel významným dodavatelem, příp. provozovatelem systému.

Ve smlouvě by měla být v co největších podrobnostech popsána jednotlivá práva a povinnosti smluvních stran co do způsobů realizace relevantních bezpečnostních opatření podle § 5 ZKB a určena odpovědnost za řádné plnění jednotlivých bezpečnostních opatření. Obecné deklarace v tom smyslu, že dodavatel je odpovědný za dodržování ZKB a VKB bez další konkretizace, jsou nedostatečné.

Smlouva s dodavatelem dále obsahuje popis úrovně služeb (tzv. SLA). Pro konkrétní případ se stanovují takové parametry úrovně služeb, které zohlední povahu plnění smlouvy.

Smlouva by měla dále obsahovat:

- vymezení úrovně poskytovaných služeb,
- způsob komunikace pro řízení kybernetických bezpečnostních událostí a incidentů,
- způsob a úroveň realizace jednotlivých bezpečnostních opatření,

- podmínky výkonu kontrolní činnosti ze strany organizace zaměřené na dodržování stanovených bezpečnostních opatření dodavatelem,
- povinnost dodavatele realizovat nápravná opatření z kontrolní činnosti organizace,
- určení vzájemné smluvní odpovědnosti v oblasti kybernetické bezpečnosti,
- výši sankcí za porušení povinností v oblasti kybernetické bezpečnosti,
- pravidla náhrady škody,
- pravidla pro řízení dokumentace,
- pravidla při ukončení smluvního vztahu (tzv. exit plan).

Požadavky na obsah smluv s významnými dodavateli jsou uvedeny v příloze č. 7 VKB, pro ostatní dodavatele se jedná o doporučená ustanovení.

Následující výčet uvádí hlavní oblasti, které mohou být pro objednatele při identifikaci jeho požadavků na smlouvy klíčové.

Předmět zakázky:

- detailní specifikace rozsahu a úrovně požadovaného předmětu plnění,
- určení místa a času požadovaného plnění,
- stanovení časového rámce, ve kterém bude plnění poskytováno,
- specifikace funkcionality předmětu plnění,
- stanovení počtu uživatelů požadujících předmět plnění,
- specifikace předmětného hardwaru a softwaru,
- specifikace vývoje a procesů řízení změn,
- nastavení úrovně dostupnosti systémů a aplikací,
- nastavení integrity zpracování,
- nastavení rozhraní s ostatními systémy.

Service Level Agreement (SLA):

- popis provozu služby, včetně údržby a servisních služeb,
- dostupnost systémů (včetně vyhodnocovacího období),
- úrovně údržby, doplňovací cyklus,
- reakční časy (do kdy je nutné zahájit řešení problému),
- čas řešení problémů (RTO – doba, do které je nutné obnovit provoz),
- garantovaná doba dostupnosti,
- nejdelší doba výpadku,
- termíny a časy fungování systémů a podpory,
- klíčové rizikové ukazatele týkající se důvěrnosti, dostupnosti a integrity informací,
- klíčové rizikové ukazatele týkající se činností dodavatele, jež mají nebo mohou mít dopad na organizaci,
- frekvence monitoringu a hlášení,
- postup v případě porušení výše uvedeného (eskalační proces), pokuty a sankce.

Bezpečnost:

- stanovení úrovně bezpečnosti informací z pohledu důvěrnosti, dostupnosti a integrity,
- určení způsobu a výše úhrady účelně vynaložených nákladů na zavedení bezpečnostních pravidel,

- stanovení ochrany systémů a informačních aktiv prostřednictvím obnovy záloh, plánování pro případy nepředvídatelných událostí nebo propouštění,
- ustanovení o povinnosti dodavatele informovat objednatele o incidentech souvisejících s plněním smlouvy,
- ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky objednatele nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele objednatelem,
- monitoringu aktiv a souvisejících dat, odezva (objednatele i dodavatele) a postupy oznamování (rutinního i incidentů),
- ekonomické spolehlivosti dodavatele,
- přístupu dodavatele k informacím objednatele, které jsou přenášeny prostřednictvím jejich komunikačních systémů a aplikací,
- definování a úpravy systému schvalování pro případy poddodávek prováděných třetími stranami,
- ustanovení upravující řetězení dodavatelů, přičemž musí být zajištěno, že poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi povinnou osobou a dodavatelem a nebudou v rozporu s požadavky povinné osoby na dodavatele,
- povinnost dodavatele informovat povinnou osobu a způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy.

Komunikace:

- rozvržení systému komunikace mezi objednatelem a dodavatelem,
- implementace ustanovení o součinnosti, i s případnými sankcemi při neposkytnutí součinnosti.

Data:

- určení vlastnictví dat a oprávnění užívat data,
- specifikace vlastnictví informačních aktiv, včetně dat a doménových jmen,
- doba uchování zálohovaných dat organizace,
- ochrana přístupu uživatele k úložišti dat (popisuje mechanismy používané k ochraně pověření uživatele pro přístup k službám),
- specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání správcem,
- pravidla pro likvidaci dat.

Záruky a odpovědnost:

- zavedení záruk dodavatele za kvalitu jím nebo třetí stranou poskytované služby,
- odpovědnosti za design, implementaci, výkonnost a monitoring kontroly,
- odpovědnosti za data, ochranu osobních údajů a soukromí,
- odpovědnosti za systém, komunikaci, operační systém, pomocný software, data a kontrolu přístupů do aplikačního softwaru a jejich správu,
- ustanovení o způsobu převzetí smluv s třetími stranami.

Právo na audit:

- kdo může vykonávat audit (zda např. zaměstnanec objednatele, kdokoliv, kdo je zmocněn objednatelem, nebo případně jiný subjekt),
- jak často se může audit opakovat a délka jeho trvání,
- náklady na audit a jejich hrazení,
- možnost setkat se s pracovníky interního auditu dodavatele a přezkoumat jejich auditní práci a výstupy auditu,

- oznámení doby provedení auditu a způsob tohoto oznámení,
- požadavky na dokumentaci.

Přezkoumávání smlouvy:

- ustanovení o pravidelném přezkoumávání předmětu smlouvu, souladu s aktuálními požadavky a z toho vyplývajících změn smlouvy.

Řízení změn:

- ustanovení o pravidlech schvalování změn obsahu smlouvy;
- stanovení přezkumu možných dopadů změn (např. prostřednictvím hodnocení rizik), akceptačního procesu (jakým způsobem je změna přijata), testování před nasazením do provozu, promítnutí do bezpečnostních politik, dokumentování změny, možnost navrácení do původního stavu apod.,
- povinnost dodavatele informovat objednatele o významné změně ovládání tohoto dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, případě změně oprávnění nakládat s těmito aktivy, využívaných tímto dodavatelem k plnění podle smlouvy
  se správcem.

Právo duševního vlastnictví:

- ustanovení o autorství programového (zdrojového) kódu, popřípadě o programových licencích.

Mlčenlivost (NDA):

- ustanovení o zachování mlčenlivosti (důvěrnosti) informací souvisejících se smlouvou.

Soulad s právními předpisy:

- ustanovení o souladu smluv s obecně závaznými právními předpisy,
- postup v případě významných legislativních změn a způsob, jakým bude těmto požadavkům smlouva přizpůsobena.

Ukončení smlouvy a řešení sporů:

- okolnosti, za kterých může být smlouva ukončena,
- smluvní pokuty v případě ukončení za jiných než stanovených okolností,
- lhůty, ve kterých je potřeba takové ukončení smlouvy provést,
- podmínky pro obnovení smlouvy, včetně vyjednávacích procesů,
- prověření a odsouhlasení změn smlouvy a souvisejících dokumentů (např. SLA),
- specifikaci podmínek ukončení smlouvy z pohledu bezpečnosti (např. exit strategie, pravidla předání dat a informací, formát předávaných dat, likvidace předaných dat nebo finanční aspekty předání dat),
- specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli (například zahrnutí dodavatelů do havarijních plánů, úkoly dodavatelů při aktivaci řízení kontinuity činností),
- ustanovení o právu jednostranně odstoupit od smlouvy v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle smlouvy,
- ustanovení o sankcích za porušení povinností.

Pravidla pro provádění kontroly zavedení bezpečnostních opatření

Kontrola zavedení a dodržování bezpečnostních opatření dodavatelem je součástí hodnocení rizik dodavatelů.

Kontrolní mechanismy:

- bezpečnostní audit u dodavatele před uzavřením smluvního vztahu,

- bezpečnostní audit u dodavatele po implementaci požadovaných bezpečnostních opatření,
- výkon plánovaných nebo nahodilých kontrol,
- následné kontroly k ověření realizace nápravných opatření,
- sledování dodržovaní smluvně stanovené úrovně služeb.

Kontrola v průběhu smlouvy

U uzavřených smluv musí být pravidelně prováděna kontrola bezpečnostních opatření prostřednictvím přezkoumávání plnění smluv v rozsahu dodržování požadavků na bezpečnostní opatření, a to:

- u významného dodavatele alespoň jednou za půl roku,
- u dodavatele alespoň jednou za rok.

V průběhu trvání smluvního vztahu musí být průběžně kontrolováno a monitorováno jeho plnění přiměřeně s ohledem na důležitost dodávky. Za přezkoumávání je odpovědný obvykle zaměstnanec odpovědný za smluvní vztah a auditor kybernetické bezpečnosti.

Předmětem kontroly bude zejména:

- zajištění důvěrnosti, dostupnosti a integrity informací,
- postupy předávání informací třetím stranám,
- dodržování podmínek SLA,
- vyhodnocování dodržování SLA z pohledu dodavatele,
- aktuálnosti jmenného seznamu zaměstnanců dodavatele, kteří budou přistupovat k datům nebo službám odběratele, včetně způsobu seznámení těchto zaměstnanců s bezpečnostními pravidly,
- výsledky spojené s monitorováním výkonnosti, kvality a bezpečnosti služeb a řídicích systémů a míry plnění dohody o bezpečnosti služby,
- přezkoumání zpráv o službách poskytovaných dodavatelem a výsledky pravidelných setkání s dodavatelem,
- výsledky auditů, které se k danému dodavateli vztahují a přístup dodavatele k řešení nálezů,
- výsledky řešení kybernetických bezpečnostních incidentů, přístup dodavatele k řízení kybernetických bezpečnostních incidentů a stav opatření k zamezení opakování kybernetických bezpečnostních incidentů,
- záznamy, které se vztahují k bezpečnosti informací souvisejících s dodavatelem, jako jsou události bezpečnosti informací, provozní problémy, selhání nebo výpadky vztahující se ke službám poskytovaným dodavatelem,
- výsledky činností spojených s aktivací nebo testováním plánů kontinuity a schopnosti dodavatele naplnit cíle kontinuity a související ujednání,
- aktualizace hodnocení rizik souvisejících s dodavatelem v souhrnném hodnocení rizik,
- řízení poddodavatelů dodavatele,
- kontrola shody se smlouvou,
- evidence, řízení a řešení všech identifikovaných problémů,
- evidence, řízení a řešení změn, včetně provedení analýzy k provedení změny.

O reportech a závěrech musí být informován manažer kybernetické bezpečnosti. Na základě zjištěných nedostatků musí být přijímána efektivní bezpečnostní opatření pro jejich řešení. Zároveň je smluvně upraven postup pro řešení změn na straně dodavatele, resp. pro zavádění bezpečnostních opatření pro napravení nedostatků.

Pravidla pro provádění zákaznického auditu u dodavatele

V případě, že dojde k potřebě provést zákaznický audit, je proveden přiměřeně podle vnitřního předpisu pro audit kybernetické bezpečnosti podle § 16 VKB a její přílohy č. 5: 1.1. Pravidla a postupy

pro provádění auditů kybernetické bezpečnosti, anebo prostřednictvím externí společnosti. Rozsah auditu je dán požadavky na daného dodavatele podle struktury dodávek či poskytovaných služeb. Periodicita, způsob a rozsah provádění auditů u dodavatele musí být upraven ve smlouvě s dodavatelem.

Součástí provádění zákaznického auditu musí být umožnění otestování:

- procesu zvládání kybernetických bezpečnostních incidentů,
- havarijních plánů a plánů kontinuity služeb dodavatele,
- bezpečnostních parametrů služby.

Příloha č. 6 Smlouvy

Nástroj pro hodnocení dodavatele dle VKB

Pravidla pro hodnocení dodavatelů

Informace o dodavatelích sloužící k jejich hodnocení jsou zaznamenávány do tabulky č. 3 Vzor tabulky hodnocení dodavatele.

Za aktuálnost a věcnou správnost evidence dodavatelů zpravidla zodpovídá manažer kybernetické bezpečnosti, za jednotlivá hodnocení dodavatelů odpovídají příslušní zaměstnanci odpovědní
za smluvní vztah. Všechny dokumenty musí být pravidelně aktualizovány odpovědnými osobami.

Informace o dodavateli jsou získávány z veřejně dostupných zdrojů, zkušenostmi s dodavatelem před, během a po ukončení smluvního vztahu, z informací příslušných orgánů a z dalších relevantních zdrojů. Mělo by jít o ověřené a legálně získané informace.

Na základě všech dostupných informací je dodavatel ohodnocen, čímž dojde ke stanovení kategorie dodavatele.

Postup při hodnocení dodavatelů

Dodavatel je obvykle hodnocen především v následujících oblastech:

- historie/pověst dodavatele,
- certifikace,
- v oblasti bezpečnosti informací,
  - v oblasti řízení jakosti,
  - reference ze spolehlivých zdrojů,
- transparentnost vlastnické struktury,
- kvalita a dostupnost informací z veřejných zdrojů,
- předchozí zkušenosti:
  - kvalita spolupráce,
  - kvalita technické podpory,
  - dodržení termínů dodávky,
  - včasné informace o změnách a jejich zdůvodnění,
  - reklamace a případné problémy s jejich uplatněním,
  - výsledky zákaznických auditů u dodavatele nebo kontrol příslušných státních orgánů,
  - dodržování smluvně stanovené úrovně poskytování služeb.

Tabulka 1: Bodové hodnocení

Počet bodů	Popis	Příklad
2	Bylo zjištěno velké množství pozitivních informací.	S dodavatelem je dlouhodobě spolupracováno bez komplikací, anebo dodavatel je spolehlivou organizací s dlouhodobou historií a množstvím kladných referencí ze spolehlivých zdrojů.
1	Bylo zjištěno menší množství pozitivních informací.	O dodavateli jsou k dispozici kladné recenze, ale nejsou dostupné žádné přímé zkušenosti nebo informace ze spolehlivých zdrojů.
0	Nebyly zjištěny žádné informace.	Dodavatel je na trhu teprve krátce, anebo nebylo možné zjistit dostatek relevantních informací, aby mohl být objektivně posouzen.
-1	Byly zjištěny drobné nedostatky.	Na dodavatele existují stížnosti, které nejsou závažného charakteru.
-2	Byly zjištěny zásadní negativní informace.	Vážné negativní zkušenosti z minulé spolupráce s dodavatelem, anebo jejich detailní popis ze spolehlivého zdroje.

Na základě bodového hodnocení dodavatele v jednotlivých oblastech je zařazen do jedné z kategorií např. podle následující tabulky:

Tabulka 2: Kategorie dodavatelů

Počet bodů	Kategorie	Popis
12 až 22	**A**	Pro řízení dodavatele stačí standardní pravidla řízení dodavatelů, která jsou shodná pro všechny.
0 až 11	**B**	K řízení dodavatele jsou doporučena méně náročná bezpečnostní opatření nad rámec standardních pravidel, v případě vyšší náročnosti opatření lze dodavatele řídit s využitím pouze standardních pravidel.
-11 až -1	**C**	K řízení dodavatele je potřeba zavést další bezpečnostní opatření nad rámec standardních pravidel.
-22 až -12	**D**	Dodavatel je považován za nevhodného a není doporučen ke spolupráci.

Hodnocení může být sestaveno i např. na základě dotazníku, ve kterém je stanovena sada požadavků vycházejících ze ZKB, příp. z normy ČSN ISO/IEC 27001. Dodavatel následně dotazník vyplní a výsledek může být podkladem pro hodnocení dodavatele ve formě bodového ohodnocení. Alternativně může být využito i předložení auditorské zprávy nezávislé externí auditorské společnosti za účelem ověření souladu implementovaného kontrolního rámce, dodržování bezpečnostních kontrol, opatření, procesů a systému řízení bezpečnosti informací podle požadavků a opatření vyplývajících z ČSN ISO/IEC 27001 (ISO 27002) a ZKB, v oblasti řízení informační bezpečnosti a ochrany informací.

Další možností je dodání nezávislého reportu externího hodnotitele jako např. ISAE 3402, SSAE 18, který provedl posouzení prostředí dodavatele obsahující přehled přijatelných bezpečnostních kontrol, opatření a postupů pro řízení bezpečnosti informací a řízení a zvládání rizik a incidentů.

Hodnocení dodavatelů je prováděno před uzavřením smlouvy a po ukončení smlouvy, protože může sloužit jako podklad pro budoucí smluvní vztahy, příp. jako podklad jiné části organizace, která by chtěla s dodavatelem spolupracovat. V průběhu smluvního vztahu jsou prováděna průběžná hodnocení, která slouží jako podklad pro hodnocení dodavatele po ukončení smluvního vztahu. Průběžná hodnocení se nemusí pokaždé týkat všech oblastí hodnocení dodavatele, ale musí obsahovat všechny relevantní skutečnosti z průběhu smluvního vztahu. Průběžná hodnocení, jako např. poznámky o zpoždění dodávky, jsou prováděna ideálně jednou za půl roku. Za provedení hodnocení odpovídá zaměstnanec odpovědný za smluvní vztah.

Zaměstnanci odpovědní za smluvní vztah se podílejí na zlepšování procesu hodnocení dodavatelů obvykle společně s manažerem kybernetické bezpečnosti.

Využití výstupů hodnocení dodavatelů

O výsledku hodnocení dodavatele je informován manažer kybernetické bezpečnosti. Negativní hodnocení dodavatele v oblasti kybernetické bezpečnosti by mělo být projednáno výborem pro řízení kybernetické bezpečnosti.

Na základě zjištěné míry rizika přijímá osoba odpovědná za řízení rizik a akceptaci v organizaci příslušná bezpečnostní opatření před uzavřením smlouvy nebo v rámci již uzavřených smluvních vztahů.

Hodnocení může být prakticky využito při výběru dodavatelů do nových smluvních vztahů. Pozitivně hodnocený dodavatel může být na základě hodnocení upřednostněn, naopak negativní hodnocení může být důvodem vyřazení dodavatele jednak při uzavírání smluvního vztahu mimo režim ZZVZ, příp. i při hodnocení nabídek v rámci ZZVZ. V takovém případě lze u účastníka zvážit vyloučení ze zadávacího řízení na základě § 48 odst. 5 písm. d) ZZVZ.

Kontrola účinnosti řízení dodavatelů

Za účelem neustálého zlepšování musí být prováděna kontrola účinnosti procesu řízení dodavatelů alespoň jednou za rok. Za kontrolu účinnosti řízení dodavatelů obvykle odpovídá manažer kybernetické bezpečnosti, který spolupracuje s jednotlivými zaměstnanci odpovědnými za smluvní vztahy za účelem zlepšení procesů.

Kontrola účinnosti je zaměřena na:

- provádění identifikace a hodnocení rizik souvisejících s dodávaným plněním,
- provádění identifikace a hodnocení rizik souvisejících s dodavateli,

- vedení a aktualizování evidence dodavatelů,
- promítnutí bezpečnostních požadavků do smluv s dodavateli,
- zohledňování hodnocení dodavatelů do výběru dodavatele,
- seznamování a kontrolu dodržování bezpečnostních opatření dodavateli (např. zákaznický audit).

Výsledkem kontroly účinnosti procesu řízení dodavatelů je zpráva o účinnosti, která obsahuje zjištění a doporučení pro zlepšení celého procesu.

Zpráva o účinnosti je jedním ze vstupních zdrojů informací pro celkové vyhodnocení účinnosti systému řízení bezpečnosti informací a její výsledky musí být zohledněny v plánu zvládání rizik.

Tabulka 3. Vzor tabulky hodnocení dodavatele

HODNOCENÍ DODAVATELE		
Hodnotil:		
Datum hodnocení:		
Základní informace o dodavateli		
Název subjektu (firma):		
IČ:		
Adresa (sídlo):		
Statutární zástupce:		
Právní forma:		
Základní kapitál:		
Oblast hodnocení	**Počet bodů**	**Komentář**
Historie/pověst dodavatele:		
Certifikace:		
Reference ze spolehlivých zdrojů:		
Transparentnost vlastnické struktury:		
Kvalita a dostupnost informací z veřejných zdrojů:		
Předchozí zkušenosti:		
kvalita spolupráce		
kvalita technické podpory		
dodržení termínů dodávky		
včasné informace o změnách a jejich zdůvodnění		
reklamace a případné problémy s jejich uplatněním		
výsledky zákaznických auditů u dodavatele		
Výsledek hodnocení		
Celkový počet bodů:	**0**	
Zařazen do kategorie:	**B**	

Tabulka č. 4 Vzor souhrnné tabulky hodnocení dodavatelů

Informační systém	ID dodavatele	Název dodavatele	Typ dodavatele	Identifikace smlouvy	Datum hodnocení dodavatele	Odkaz na formulář	Zaměstnanec odpovědný za smluvní vztah	Kategorie dodavatele	Datum informování významného dodavatele	Datum posledního zákaznického auditu	Odkaz na zprávu ze zákaznického auditu	Poznámka
IS001	1	ABC a.s.	významný dodavatel		06.02.2020			A	10.02.2020			VZOR
IS002	2	DEF s.r.o.	dodavatel		07.02.2020			C	N/A			VZOR
IS002	3	XYZ a.s.	provozovatel		06.02.2020			B	12.02.2020			VZOR

Příloha č. 7 Smlouvy

Zachování kontinuity podpory

Zachováním kontinuity podpory se rozumí nastavení režimu zpracování a vypořádání již zadaných požadavků na úpravy a dopracování funkcionalit systému UNIS do systému helpdesku dodavatele.

Zadané a evidované požadavky zadavatele jsou rozděleny do kategorií priorit z hlediska vypořádání:

Priorita 1 – Vysoká – dodavatel garantuje vypořádání požadavku nejpozději do 6 měsíců od data započetí platnosti smlouvy. Po uplynutí doby 6 měsíců nevypořádaný požadavek s touto prioritou okamžitě do stavu prodlení plnění a může na něj být uplatněna sankce podle aktuálně platné servisní smlouvy.

Priorita 2 – Standartní – dodavatel garantuje vypořádání požadavku nejpozději do 9 měsíců od data započetí platnosti smlouvy. Po uplynutí doby 9 měsíců a 60 kalendářních dnů nevypořádaný požadavek s touto prioritou okamžitě do stavu prodlení plnění a může na něj být uplatněna sankce podle aktuálně platné servisní smlouvy.

Priorita 3 – Nízká – dodavatel garantuje vypořádání požadavku nejpozději do 12 měsíců od data započetí platnosti smlouvy. Po uplynutí doby 12 měsíců a 60 kalendářních dnů nevypořádaný požadavek s touto prioritou okamžitě do stavu prodlení plnění a může na něj být uplatněna sankce podle aktuálně platné servisní smlouvy.

Priorita 4 – Odloženo k další analýze (nemá určený termín řešení, ale požadavek nadále zůstává zadaný v HD)

Priorita 5 – zrušený požadavek (požadavek, který se vyřešil jiným způsobem nebo ho není třeba již řešit a bude v HD ukončen)

Přehled evidovaných požadavků k datu 14.4.2023 je uveden v Tabulce 1

Příloha č. 8 Smlouvy

Metodika hodnocení rizik

Metodika slouží jako podklad pro zpracování analýzy a řízení rizik v kontextu systému řízení bezpečnosti informací, popisuje principy, na kterých je analýza a řízení rizik založena, definuje rozsah zapojení a odpovědnost jednotlivých rolí a použité nástroje a postupy.

Metodika analýzy a řízení rizik se vztahuje na všechny informace, které jsou uloženy, spravovány nebo používány v Univerzálním nemocničním informační systému UNIS, bez ohledu na formu, formát, nosné médium, nebo zda se jedná o zpracování automatizované nebo ruční.

Metodika analýzy a řízení rizik se dále vztahuje na všechny zdroje používané pro tvorbu, zpracování, přenos, ukládání, užívání a kontrolu těchto informací.

Metodika analýzy a řízení rizik je v souladu s obecně závaznými právními předpisy, vnitřními předpisy FN Motol, se zásadami kybernetické bezpečnosti FN Motol, s bezpečnostní politikou informací MZ ČR a s požadavky definovanými v zákoně č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen ZKB) a vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů

Definice

Architekt kybernetické bezpečnosti navrhuje základní bezpečnostní architekturu informačních a komunikačních systémů, jejich jednotlivých komponent, vzájemných vazeb a dohlíží na soulad implementace architektury informačních a komunikačních systémů se systémem řízení kybernetické bezpečnosti.

Auditor kybernetické bezpečnosti provádí audity systému řízení kybernetické bezpečnosti a kontroluje dodržování pravidel kybernetické bezpečnosti.

Garant podpůrného aktiva je fyzická osoba pověřená k zajištění provozu, rozvoji, použití a bezpečnosti technického aktiva. Garantem podpůrného aktiva jsou administrátoři, techničtí správci serverů, sítě apod., tj. osoby odpovědné za chod zařízení při dodržení nastavených parametrů poskytovaných služeb.

Garant primárního aktiva je fyzická osoba pověřená k zajištění rozvoje, použití a bezpečnosti primárního aktiva. Garant primárního aktiva je odpovědný za provoz aktiva po obsahové stránce.

Informace jsou data (bez ohledu na to, zda jsou uložena centrálně, nebo distribuovaná).

Informační aktiva (dále jen aktiva) jsou informace, zařízení nebo programy, na kterých je organizace závislá při zajišťování svého předmětu činnosti. Především se jedná o data v informačních systémech, dokumentech organizace a jejich zálohách.

Manažer kybernetické bezpečnosti je pracovník, který odpovídá za systém řízení kybernetické bezpečnosti.

Perimetr je hranice oblasti, po kterou je zajišťována kybernetická bezpečnost informačních systémů FN Motol.

Podpůrná aktiva jsou HW, SW, počítačové sítě, pracovníci, lokalita, dodavatelé apod., na kterých jsou primární aktiva závislá.

Počítačový vir je program, který se dokáže v počítači sám šířit bez vědomí uživatele a poškodit data, software nebo odesílat uživatelské údaje

Primární aktiva jsou informace nebo služby, které zpracovávají nebo poskytují informační systémy. V případě, že dojde k narušení primárního aktiva, nemocnice nemůže vykonávat zdravotnické činnosti.

Služby jsou funkce, které uživatelům umožňují přístup a práci s daty (pořizování, ukládání / uchování - včetně tvorby kopií, přenos, transformace / modifikace (změny

formátu, šifrování, mazání), prezentace (digitální publikování na webových stránkách, promítání) nebo jejich tisk.

Spyware je program, který využívá internetové stránky k odesílání dat z počítače (či mobilního telefonu nebo jiného zařízení) bez vědomí jeho uživatele (např. přehled navštívených stránek či nainstalovaných programů, hesla a čísla kreditních karet).

Trojský kůň je uživateli skrytá část počítačového programu nebo aplikace s funkcí, se kterou uživatel nesouhlasí (typicky je to činnost škodlivá). Trojský kůň může být samostatný program, který se tváří užitečně – například hra, spořič obrazovky nebo nějaký jednoduchý nástroj, ale jeho funkčnost slouží jako maskování záškodnické činnosti, kterou v sobě trojský kůň ukrývá.

Výbor pro řízení kybernetické bezpečnosti je nejvyšší orgán pro oblast kybernetické bezpečnosti, který řídí a kontroluje dodržování pravidel kybernetické bezpečnosti.

Zkratky

ČR	Česká republika
EU	Evropská unie
FN Motol	Fakultní nemocnice v Motole
GDPR	Nařízení 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)
HW (hardware)	Servery, disková pole, koncová zařízení (počítače, notebooky), síťové prvky
KB	Kybernetická bezpečnost
MZ ČR	Ministerstvo zdravotnictví České republiky
SW (software)	Počítačové programové vybavení
UNIS	Univerzální nemocniční informační systém
VKB	Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů
ZKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

Vstupní dokumentace

- Identifikace a analýza informačních aktiv
- Dokumentace z předchozí analýzy rizik:
  - zpráva o hodnocení aktiv a rizik – identifikace rizik,
  - analýza (ohodnocení rizik) - posouzení možných dopadů hrozeb a zranitelností na aktiva,
  - zpráva o stanovení kritérií přijatelnosti rizik včetně stanovení přijatelné míry zbytkového rizika,
  - určení a schválení přijatelných rizik včetně stanovení (ne)přijatelné míry (akceptace rizik).

Výstupní dokumentace

Výstupem analýzy rizik jsou následující dokumenty:

- **analýza rizik** pro účely funkcí zajišťujících systém řízení informační bezpečnosti,
- **prohlášení o aplikovatelnosti** obsahující přehled zavedených bezpečnostních opatření,
- **plán zvládání rizik** obsahující cíle a přínosy bezpečnostních opatření pro zvládání rizik, určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení a popis vazeb mezi riziky
  a příslušnými bezpečnostními opatřeními.

Rozsah analýzy rizik

Analýza rizik se zabývá stanovením míry rizika ve vztahu k jednotlivým aktivům v rámci rozsahu systému řízení bezpečnosti informací.

Hlediska hodnocení

Zahrnutí aktiva, systému či útvaru do bezpečnostního perimetru musí být hodnoceno podle hledisek:

- bezpečnostní vazby mezi systémy,
- vliv pracovníků na bezpečnost informací,
- hodnota aktiva

Proces stanovení rozsahu analýzy rizik

- předběžné stanovení rozsahu analýzy rizik
- identifikace a hodnocení aktiv nad rozsahem definovaným v předchozím kroku,
- porovnání výsledků identifikace a hodnocení aktiv s předběžně stanoveným rozsahem,
- provedení korekce rozsahu,
- identifikace a hodnocení aktiv nad korigovaným rozsahem,
- identifikace podpůrných aktiv s ohledem na bezpečnostní vazby mezi systémy, které by mohly ovlivnit úroveň bezpečnostních opatření prostřednictvím jejich sdílení s ostatními prvky kybernetické bezpečnosti ve FN Motol.

Zpracování analýzy rizik

Metodika definuje postup s užitím kvalitativních měřítek. Kvalitativní analýza rizik je založena na expertním odhadu míry zranitelností a hrozeb pro jednotlivá aktiva a hodnocení jejich dopadů.

Identifikace a hodnocení zranitelností

Každé identifikované aktivum má určité zranitelnosti, které mohou vést k poškození aktiv a tím k porušení jeho dostupnosti, důvěrnosti či integrity. Tyto zranitelnosti se identifikují pro aktiva ve stavu, bez již přijatých bezpečnostních opatření.

Identifikaci zranitelností a jejich zdrojů provede manažer kybernetické bezpečnosti ve spolupráci s garanty jednotlivých aktiv tak, že pojmenují zranitelnosti, která mohou aktiva ohrozit.

Pro identifikaci zranitelností užije manažer kybernetické bezpečnosti informace o vadách a slabinách aktiv z veřejně dostupných zdrojů, z provozní a technické dokumentace, z provozních zkušeností s daným aktivem a z dříve provedených bezpečnostních analýz. Na základě vyhodnocení těchto podkladů zpracuje manažer kybernetické bezpečnosti seznam bezpečnostních kritérií pro jednotlivé oblasti bezpečnosti (uživatelská, provozní a technická).

Pro části systému, které jsou ve fázi vývoje, musí být identifikace zranitelností zaměřena na bezpečnost systému, předpokládané bezpečnostní postupy, vymezení požadavků na systém a analýzu bezpečnosti vydanou výrobcem.

Pro části systému, které jsou ve fázi implementace, musí identifikace zranitelností zahrnovat vlastnosti plánované bezpečnosti, které jsou popsané v bezpečnostní dokumentaci systému, výsledky certifikace, testů a jejich vyhodnocení.

Pro provozované části systémů musí identifikace zranitelností zahrnovat analýzu vlastností systémové bezpečnosti, management bezpečnosti včetně technik a procesů užitých k ochraně systému.

Při hodnocení musí být zohledněny i zkušenosti z bezpečnostních incidentů předchozích hodnocení zranitelností.

Identifikované hrozby jsou uspořádány a seskupeny hierarchicky a to po skupinách zranitelností, jež mají společný zdroj zranitelností.

Základní charakteristikou zranitelnosti je její úroveň, která se hodnotí podle následujících faktorů:

- citlivost aktiva, která vyjadřuje jeho náchylnost být daným nebezpečím poškozeno,
- kritičnost aktiva, která vyjadřuje důležitost aktiva pro analyzovaný systém či subjekt.

Každé aktivum musí být prověřeno z hlediska možné hrozby z pohledu dostupnosti, důvěrnosti a integrity.

Seznam zranitelností musí být průběžně doplňován a opakovaně validován při každé revizi analýzy rizik, jakož i v případě změny podmínek, jež platná analýza ošetřuje.

Seznam nejvýznamnějších zranitelností:

a) nedostatečná údržba informačního a komunikačního systému,
b) zastaralost informačního a komunikačního systému,
c) nedostatečná ochrana vnějšího perimetru,
d) nedostatečné bezpečnostní povědomí uživatelů a administrátorů,
e) nedostatečná údržba informačního a komunikačního systému,
f) nevhodné nastavení přístupových oprávnění,
g) nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
h) nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování,
i) nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí,
j) nedostatečná ochrana aktiv,
k) nevhodná bezpečnostní architektura,
l) nedostatečná míra nezávislé kontroly,
m) neschopnost včasného odhalení pochybení ze strany zaměstnanců.

Tabulka č. 2 - Stupnice pro hodnocení zranitelností

Úroveň		Popis hodnocení zranitelností
1	Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.
2	Střední	Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
3	Vysoká	Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
4	Kritická	Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté. Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Identifikace a hodnocení hrozeb

Hrozba má potenciál poškodit aktiva jako jsou informace, procesy a systémy, tedy poškodit informační systémy FN Motol. Hrozby mohou být přírodního nebo lidského původu a mohou být náhodné nebo úmyslné.

Identifikace hrozeb a jejich zdrojů provede manažer kybernetické bezpečnosti ve spolupráci s garanty aktiv tak, že pojmenuje hrozby a jejich zdroje, které mohou aktiva ohrozit.

Při identifikaci hrozeb musí být zohledněny rovněž hrozby vyplývající ze statutu FN Motol, postavení na trhu, hospodářských výsledků a další specifické atributy.

Hrozby budou identifikovány podle typu (například neoprávněné akce, fyzické zničení, technické poruchy) a následně, budou v rámci obecné třídy identifikovány jednotlivé hrozby do úrovně detailu potřebného pro následné určení míry rizika a příslušných protiopatření.

Některé hrozby mohou postihnout více než jedno aktivum. V takových případech mohou mít různý dopad v závislosti na tom, která aktiva jsou postižena. Vstup k identifikaci hrozby a odhad pravděpodobnosti výskytu určí garanti nebo uživatelé aktiv, pracovníci lidských zdrojů, manažer kybernetické bezpečnosti, experti v oblasti fyzické bezpečnosti a právní oddělení.

Při hodnocení musí být zohledněny zkušenosti z bezpečnostních incidentů a minulých hodnocení hrozeb.

Při použití výsledků dřívějších hodnocení hrozeb musí být zohledněno, že se významné hrozby mohou měnit, zejména pokud se mění okolní prostředí nebo informační systémy.

Pro účely řízení systému informační bezpečnosti vytvoří manažer kybernetické bezpečnosti ve spolupráci s garanty aktiv katalog hrozeb. Hrozby musí být identifikovány ve vztahu k aktivům, jejichž stav jsou způsobilé ovlivnit. Při posuzování hrozby musí být zohledněny i následné dopady hrozby.

Hrozby evidované v katalogu musí být uspořádány a seskupeny hierarchicky, a to po skupinách hrozeb, jež mají společný skupinový zdroj hrozeb.

Všechny evidované hrozby budou samostatně pro každou iteraci posuzovány z pohledu požadavků na zajištění důvěrnosti, integrity a dostupnosti aktiva.

Každé aktivum musí být posuzováno z hlediska hrozby a možných vlivů na všechna jednotlivá aktiva i skupiny aktiv a to vždy z pohledu zajištění důvěrnosti, integrity a dostupnosti aktiva.

Hrozby musí být doplňovány průběžně a opakovaně validovány v každé revizi analýzy rizik a v případě změny podmínek, jež platná analýza ošetřuje.

Manažer kybernetické bezpečnosti zpracuje popis stávajících opatření, která již byla přijata pro eliminaci hrozeb či snížení dopadu jejich výskytu. Opatření musí být popsána dle reálného stavu technicko - organizačních i procesních pravidel FN Motol.

Po zpracování popisu stávajících opatření, provede manažer kybernetické bezpečnosti ve spolupráci s garanty aktiv hodnocení pravděpodobnosti výskytu hrozby, resp. jejího ovlivnění dostupnosti, důvěrnosti či integrity aktiva. Hodnotí se situace, kdy hrozba využije zranitelnosti aktiva, a to pro každou identifikovanou dvojici zranitelnost – hrozba.

Seznam hrozeb:

a) porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,
b) poškození nebo selhání technického anebo programového vybavení,
c) zneužití identity,
d) užívání programového vybavení v rozporu s licenčními podmínkami,
e) škodlivý kód (například viry, spyware, trojské koně),
f) narušení fyzické bezpečnosti,
g) přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie,
h) zneužití nebo neoprávněná modifikace údajů,
i) ztráta, odcizení nebo poškození aktiva,
j) nedodržení smluvního závazku ze strany dodavatele,
k) pochybení ze strany zaměstnanců,
l) zneužití vnitřních prostředků, sabotáž,
m) dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb,
n) nedostatek zaměstnanců s potřebnou odbornou úrovní,
o) cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik,
p) zneužití vyměnitelných technických nosičů dat,
q) napadení elektronické komunikace (odposlech, modifikace).

Tabulka č. 3 - Stupnice pro hodnocení hrozeb

Úroveň		Popis hodnocení hrozeb
1	Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.

2	Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
3	Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
4	Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Hodnocení dopadu

Ovlivnění dostupnosti, důvěrnosti či integrity aktiva se hodnotí samostatně pro každý výskyt spojení aktivum + hrozba + zranitelnost.

Tabulka č. 4 - Stupnice hodnocení dopadů

Úroveň		Popis dopadu
1	Nízká	Dopad je v omezeném časovém období a malého rozsahu a není katastrofický. Rozsah případných škod nepřesahuje: a) 5 zraněných osob s následnou hospitalizací po dobu delší než 24 hodin nebo b) finanční nebo materiální ztráty do 1 000 000 Kč nebo c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího nejvýše 100 osob.
2	Střední	Dopad je omezeného rozsahu a v omezeném časovém období. Rozsah případných škod se pohybuje v rozmezí: a) do 3 osob s vážným ohrožením života nebo od 6 do 40 osob s následnou hospitalizací po dobu delší než 24 hodin nebo b) finanční nebo materiální ztráty od 1 000 000 Kč do 10 000 000 Kč nebo c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího od 100 do 600 osob.
3	Vysoká	Dopad je omezeného rozsahu, ale trvalý nebo katastrofický. Rozsah případných škod se pohybuje v rozmezí: a) od 4 do 50 osob s vážným ohrožením života nebo od 41 do 100 osob s následnou hospitalizací po dobu delší než 24 hodin nebo b) finanční nebo materiální ztráty od 10 000 000 Kč do 500 000 000 Kč nebo c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího od 600 do 2 500 osob.
4	Kritická	Dopad je plošný rozsahem, trvalý a katastrofický. Rozsah případných škod se pohybuje v rozmezí: a) 51 a více osob s vážným ohrožením života a 101 a více osob s následnou hospitalizací po dobu delší než 24 hodin nebo b) finanční nebo materiální ztráty převyšující 500 000 000 Kč anebo c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 2 500 osob.

Výpočet míry rizika

Mírou rizika je míra možnosti nepříznivé odchylky od požadovaného výsledku. Pro výpočet se použije vzorec:

$$\mathbf{R_1 = HA_1 \times P_1 \times D_1}$$

kde: R_1 je míra rizika pro aktivum 1

HA_1 je hodnota aktiva

P_1 je pravděpodobnost využití zranitelnosti hrozbou pro aktivum 1, která se vypočte podle vzorce (Zranitelnost + Hrozba)/2.
Hodnota Zranitelnosti se stanoví dle Tabulky č. 2 - Stupnice pro hodnocení zranitelností a hodnota Hrozby se stanoví dle Tabulky č. 3 - Stupnice pro hodnocení hrozeb. Výsledná hodnota se zaokrouhlí se na jedno desetinné místo.

D_1 je hodnocení dopadu pro aktivum 1, které se stanoví dle Tabulky č. 4 – Stupnice hodnocení dopadů

Výsledné hodnota míra rizika se zaokrouhlí na celé číslo.
Způsob výpočtu musí být aplikován na všechny aktiva, hrozby, zranitelnosti a dopady stejným způsobem.

Tabulka č. 5 – Stupnice pro hodnocení rizik

Hodnota	Úroveň	Míra rizika	Popis hodnocení míry rizika
1	Nízká	<1 - 16>	Riziko je považováno za přijatelné a nesleduje se.
2	Střední	<17 - 32>	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko přijatelné.
3	Vysoká	<33 - 48>	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.
4	Kritická	<49 - 64>	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.

Poznámka: metodika výpočtu cíleně preferuje vliv dopadu a dává mu větší význam než pravděpodobnost. Cílem je, aby sledování neunikla rizika s malou pravděpodobností, ale kritickým dopadem.

Akceptace (přijatelnost) rizik

Pokud není stanoveno jinak, rizika s hodnotou do 16 se nesledují. Rizika s hodnotou do 32 se sledují v případě, že hodnota aktiva a dopadu dosahují hodnocení 4.

Manažer kybernetické bezpečnosti ve spolupráci s garanty aktiv a architektem kybernetické bezpečnosti zpracuje návrh na opatření k eliminaci rizik, stanoví jednotnou hranici míru přijatelné míry rizika pro akceptaci (zbytkové riziko) a předloží tento návrh ke schválení Výboru pro řízení kybernetické bezpečnosti.

Výbor pro řízení kybernetické bezpečnosti buď navržená opatření pro eliminaci rizik, nebo jejích dopadů přijme nebo riziko akceptuje s uvedením důvodů, proč k této variantě přistoupil tzv. zbytkové riziko.

Manažer kybernetické bezpečnosti stanoví jednotný způsob kontroly zbytkových rizik a průběžně provádí jejich kontrolu. Výsledky kontrol předloží manažer kybernetické bezpečnosti nejméně jednou ročně Výboru pro řízení kybernetické bezpečnosti.

Sledované náležitosti rizika

K riziku se evidují položky:

a) jedinečné ID
b) zkrácený název
c) celý název složený z názvu aktiva, hrozby a zranitelnosti
d) související aktivum a jeho hodnota (odkaz)
e) vlastník rizika (vlastník aktiva)
f) související Dopad
g) související Hrozba
h) související Zranitelnost
i) nápravná opatření a jejich termíny (odkaz)
j) související incidenty (odkaz)
k) míra akceptovatelnosti rizika (cílová hodnota rizika)
l) popis rizika (komentář obsahující dopad, podmínky pravděpodobnosti apod.)

m) historie práce s rizikem.

Proces řízení rizik

Cíle procesu řízení rizik:

- zajistit, aby řízení rizik bylo evidované,
- zajistit, že rizika jsou řízena v souladu se ZKB, a ostatními bezpečnostními politikami FN Motol,
- zabránit škodám a vysokým nákladům přijetím opatření k eliminaci rizika,
- řídit provozní rozhodování v oblasti bezpečnosti na základě identifikovaných rizik a jejich pravděpodobných dopadů.

Aktualizace analýzy rizik

Manažer kybernetické bezpečnosti zajistí provedení analýzy rizik nejprve jako součást zavádění systému řízení bezpečnosti informací a poté pravidelně, nejméně jednou ročně, během provozování chráněných systémů.

Nové hodnocení rizik, aktualizace plánu zvládání rizik i prohlášení o aplikovatelnosti se musí aktualizovat po provedení jakéhokoliv rozsáhlejšího zásahu do UNIS nebo při významné změně vnějších okolností.

Evidence bezpečnostních incidentů

Manažer kybernetické bezpečnosti v souladu se zákonem ZKB a vyhláškou VKB sleduje bezpečnostní incidenty, vyhodnocuje je a je garantem hlášení dle ZKB.

Vlastníci aktiv jsou povinni hlásit všechny incidenty bezodkladně manažerovi kybernetické bezpečnosti.

V rámci evidence incidentů a jejich vyhodnocení provede manažer kybernetické bezpečnosti identifikaci na konkrétní rizika, která se uplatnila a provede přehodnocení těchto rizik s ohledem na dopady konkrétního incidentu.

Typy opatření bezpečnostních opatření

Z pohledu řízení rizik se jedná o opatření, jejichž smyslem je připravit se na aktivaci možných hrozeb a minimalizovat pravděpodobnost vzniku nepříznivé události, případně minimalizovat její dopady.

Typy opatření:

- aplikace preventivních opatření, která jsou realizována v průběhu procesu řízení rizika před jeho aktivací s cílem:
  - minimalizovat pravděpodobnost rizika přijímáním opatření, která zvyšují odolnost systému vůči identifikovaným hrozbám,
  - minimalizovat dopady, které může nepříznivá situace způsobit (např. vytvářením záloh a jejich uchovávání mimo prostory FN Motol vč. pravidelného testování plánů obnovy informačních systémů a dat),
  - přenést riziko na jiný subjekt (např. delegováním vybraných služeb na specializovaný subjekt, nebo pojištěním kritických komponent, systémů či procesů),
- opatření, která jsou zaměřena na minimalizaci dopadů v situaci, kdy se hrozba aktivovala a nepříznivá situace se stala skutečností.

Plánování a implementace bezpečnostních opatření

Po provedení analýzy rizik musí manažer kybernetické bezpečnosti vypracovat minimálně pro skupinu nejvýznamnějších rizik (rizika s největším dopadem a současně největší pravděpodobností výskytu plán zvládání rizik a předložit jej ke schválení Výboru pro řízení kybernetické bezpečnosti.

V plánu zvládání rizik musí být pro každé vybrané riziko navržena bezpečnostní opatření a posouzeny náklady a přínosy jednotlivých opatření pro chráněné aktivum a systém jako celek.

Následně po schválení plánu zvládání rizik provádí manažer kybernetické bezpečnosti kontrolu, zda jsou jednotlivá preventivní opatření realizována.

Hodnocení účinností opatření

V rámci analýzy rizik, prováděné po realizaci opatření uvedených v plánu zvládání rizik, provede manažer kybernetické bezpečnosti vyhodnocení účinnosti přijatých opatření - zda došlo ke snížení míry rizika a jeho případných negativních dopadech.

Zjištění z tohoto vyhodnocení pak slouží jako vstup do dalšího plánování opatření.

Dokumenty pro řízení rizik

V rámci procesu řízení rizik budou použity následující dokumenty:

- Katalog primárních a podpůrných aktiv, která slouží pro evidenci a analýzu aktiv a následně jako východisko pro analýzu a řízení rizik,
- katalog bezpečnostních rizik, který slouží jako evidence rizik a jejich parametrů a jako nástroj posouzení závažnosti rizika,
- katalog bezpečnostních opatření, který slouží jako znalostní báze známých postupů pro odvracení rizika a eliminaci následků nepříznivých událostí.