LICENČNÍ SMLOUVA

**Ivo Bolcek**

místem podnikání:Výškovická 636/194, 700 30 Ostrava

IČ:18111246 DIČ: CZ6209030597

bankovní spojení: Česká spořitelna

číslo účtu: 1648145389/0800

jako **poskytovatel licence** na straně jedné (dále jen „poskytovatel“)

a

**Všeobecná fakultní nemocnice v Praze**

se sídlem: U Nemocnice 499/2, 128 08 Praha 2

IČ: 000 64 165 DIČ: CZ00064165

zastoupená: prof. MUDr. Davidem Feltlem, Ph.D., MBA, ředitelem

bankovní spojení: ČNB

číslo účtu: 24035021/0710

jako **nabyvatel licence** na straně jedné (dál jen „nabyvatel“)

uzavírají dnešního dne, měsíce a roku na základě výsledku **veřejné zakázky malého rozsahu** s názvem „**Modernizace dispečinku zdravotní dopravní služby**“ **vyhlášené otevřeným řízením** dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „z. č. 134/2016 Sb.“), (dále jen „veřejná zakázka“) v souladu s ustanovením § 1746 odst. 2. zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „zákon č. 89/2012 Sb.“), tuto

**licenční smlouvu (dále jen „smlouva“)**

**I.**

**Předmět plnění smlouvy**

1. Předmětem plnění této smlouvy je závazek poskytovatele dodat SW řešení pro organizaci provozu sanitní dopravy
„Informační systém software zdravotní dopravní služby“ (**IS SW ZDS**), v rámci kterého poskytovatel:
2. Zajistí poskytování časově neomezených užívacích práv k SW řešení **IS SW ZDS** pro neomezený počet uživatelů nabyvatele (multilicence)
3. Zpracuje předimplementační analýzu minimálně v následujících oblastech:
* Pravidla a postupy pro řízení projektu a plán realizace.
* Analýza procesů řešení, přičemž bude použita nejlepší praxe implementovaného řešení zohledňující specifické potřeby jednotlivých pracovišť nabyvatele.
* Architektura technologického řešení včetně určení parametrů jednotlivých prvků.
* Analýza požadavků na integraci stávajících systémů a detailní analýza rozhraní.
* Analýza rizik navrhovaného řešení z pohledu bezpečnosti dle specifikací v příloze č. 6, kap. 1).
* Popis způsobu implementace požadavků na bezpečnost.
* Popis systému pro monitorování, logování, zálohování a obnovu řešení po havárii.
* Analýza migrace dat a určení funkcionalit informačních systémů, jež budou nahrazeny.
* Specifikace typu a rozsahu dokumentace (uživatelská, technická, administrátorská).
* Návrh a popis všech testů projektu včetně specifikace testovacích scénářů.
* Plán roll-outu, kdy roll-out musí proběhnout nejprve na testovací skupinu stanic specifikovanou nabyvatelem a po ověření funkčnosti na těchto stanicích být postupný po jednotlivých pracovištích.
* Plán školení, který musí obsahovat školení přímo na pracovišti v místě nabyvatele.
* Školení musí být jak pro uživatelské používání systému, tak jeho administrátorskou správu.
* Definice zodpovědností a přiřazení práv k záloze a obnově dat.

Při zpracování předimplementační analýzy nabyvatel poskytne poskytovateli součinnost v zajištění odborných konzultací dle přílohy č. 3 této smlouvy.

Veškerá komunikace s nabyvatelem, tzn. výstupy, dokumenty atd. budou realizovány v českém jazyce.

Procesní diagramy a infrastrukturní prostřední poskytovatel zpracuje v prostředí standardně používaném pro popis procesů a infrastruktury jako je např. Archimate 3.1, Enterprise Architekt apod.

1. Implementuje SW řešení do technologického prostředí nabyvatele následujícím postupem:
* Vytvoření testovacího prostředí v on-premise nabyvatele podle parametrů uvedených v Předimplementační analýze.
* Provedení instalace aplikace v testovacím prostředí.
* Konfigurace a úpravy aplikace v testovacím prostředí.
* Konfigurace a úpravy integračního rozhraní v testovacím prostředí.
* Testování (migrace dat, funkční testy, integrační testy, systémové testy, penetrační testy, simulace výpadků HW).
* Provedení zátěžových testů – souběžná práce minimálně 30 % uživatelů.
* Zpracování a předání dokumentace.
* Proškolení klíčových i koncových uživatelů na vlastních zmigrovaných datech; nedílnou součástí každého školení je soupis hlavních bodů školení s podpisy uživatelů, který bude předán nabyvateli.
* Proškolení správců systému a databázových specialistů na vlastních zmigrovaných datech; nedílnou součástí každého školení je soupis hlavních bodů školení s podpisy uživatelů, který bude předán nabyvateli.
* Provedení testů podle testovacích scénářů.
* Vyhodnocení testovacího provozu – incidenty, jejich řešení, následné kroky a doporučení.
* Akceptace testovacího provozu.
* Vytvoření produkčního prostředí v on-premise nabyvatele podle zpřesněných parametrů.
* Provedení migrace řešení z testovacího prostředí do produkčního, provedení testů.
* Vytvoření a nastavení systému pro monitorování, logování a zálohu dat.
* Definice a nastavení přístupových práv.
* Aktualizace dokumentace, školení a řízení změn.
* Akceptační testy nabyvatele (UAT).
* Postupný roll-out na další uživatelská pracoviště.
* Uvedení do ostrého provozu a poskytování zvýšeného dohledu.
* Finální akceptace.
1. Provede integraci se systémy nabyvatele, migraci dat a nastavení SW řešení.
2. Zpracuje dokumentaci a provede zaškolení administrátorů a uživatelů nabyvatele:
* Bezpečnostní dokumentaci dle specifikací uvedených v příloze č. 6 kap. 2),
* Uživatelské příručky,
* Administrátorskou dokumentaci,
* Provozní dokumentaci,
* Technickou dokumentaci popisující architekturu systému a integrační vazby rozhraní.

Kompletní a aktuální dokumentace k dílu dle čl. I., odst. 1, bodu e) této smlouvy bude dodána před zahájením uživatelských akceptačních testů (UAT). Poskytovatel musí zajistit verzování dokumentace.

 V rozsahu kompletní dokumentace provede poskytovatel školení pracovníků nabyvatele.

1. Poskytovatel se touto smlouvou zavazuje v rámci předmětu plnění poskytnout nabyvateli oprávnění k výkonu práva užít software (multilicenci), a to způsoby a v rozsahu stanoveném dále v této smlouvě.
2. Software dodaný v rámci předmětu plnění umožňuje aktualizaci na nejnovější verzi, poskytnutá licence se vztahuje i na aktualizované verze SW.
3. Poskytovatel se zavazuje, že dodávané technické nebo programové prostředky nesmí být prostředky, které jsou zveřejněny na stránkách Národního centra kybernetické bezpečnosti (provozované NÚKIB) jako hrozba. Veškeré poskytované služby nesmí být provozované na technických nebo programových prostředcích označených NÚKIB jako hrozba.
4. Poskytovatel je povinen neprodleně informovat objednatele prostřednictvím poskytovatelem určené odpovědné osoby: Manažera kybernetické bezpečnosti, e-mail: ManazerKB@vfn.cz, o kybernetických bezpečnostních incidentech souvisejících s implementací dodávaného řešení.
5. Nabyvatel se touto smlouvou zavazuje umožnit instalaci řádně dodaného softwaru a zaplatit sjednanou cenu za poskytnutí licence k software v souladu s podmínkami sjednanými touto smlouvou.
6. Místem plnění je sídlo nabyvatele.

**II.**

### Doba plnění

1. Poskytovatel se zavazuje dodat předmět plnění v celém jeho rozsahu dle podmínek sjednaných v této smlouvě nejpozději do 30 kalendářních dnů ode dne účinnosti smlouvy.

V případě technické připravenosti nabyvatele, v opačném případě se doba plnění o příslušný počet kalendářních dní posouvá.

1. Poskytovatel zavede při implementaci relevantní bezpečnostní, technická a organizační opatření, která zajistí dodržení důvěrnosti, integrity a dostupnosti programových prostředků proti neoprávněnému přístupu, zneužití, poškození, zranitelností či jiných aspektů ohrožující bezpečnost implementace nebo budoucího funkčního řešení.
2. Termín uvedený ve čl. II. odst. 1 smlouvy je možno prodloužit pouze po vzájemné dohodě, o které se uzavírá písemný dodatek k této smlouvě.

**III.**

**Licence k software**

1. Poskytovatel poskytuje nabyvateli nevýhradní časově neomezená užívací práva (licenci) k užití software. Licence k software je poskytována bez územního omezení.
2. Poskytovatel předá nabyvateli rovněž příslušnou dokumentaci.
3. Nabyvatel je oprávněn software užít pouze k účelu vyplývajícímu z licenční smlouvy a v souladu s určením software.
4. V případě provedení úprav (patches), aktualizací (updates), vylepšení (upgrades) či jiných změn software ze strany poskytovatele je licence poskytnuta i k takto změněnému software.
5. Poskytovatel garantuje podporu vyšších verzí webových prohlížečů.
6. Nabyvatel bere na vědomí, že software je chráněn autorským právem. Nabyvatel se zavazuje, že nebude vykonávat žádnou činnost, která by mohla jemu nebo třetím osobám umožnit neoprávněné užití software.

**IV.**

**Cena**

1. Cena za předmět plnění dle čl. I smlouvy byla sjednána ve výši:

**Celková cena bez DPH 790 000,- Kč**

**DPH 165 900,- Kč**

**Cena včetně DPH 955 900,- Kč**

 (dále jen „cena“)

1. Celková cena předmětu plnění uvedená v předchozím článku je pevnou a nejvýše přípustnou cenou předmětu plnění dle této smlouvy. Smluvní strany si ujednávají, že kupní cena za věci obstarané poskytovatelem pro účely realizace předmětu plnění je zahrnuta v ceně a cena nebude po dobu trvání této smlouvy žádným způsobem upravována a na její výši nemá žádný vliv výše vynaložených nákladů souvisejících s vývojem a aplikací software ani jakýchkoliv jiných nákladů či poplatků, k jejichž úhradě je poskytovatel na základě této smlouvy či obecně závazných právních předpisů povinen. DPH bude účtována ve výši platné při vystavení účetního dokladu.

**V.**

**Platební podmínky**

1. Nabyvatel nebude poskytovat zálohy.
2. Cena dle čl. IV. této smlouvy bude uhrazena na základě faktury – daňového dokladu (dále jen faktura) vystavené poskytovatelem, která musí obsahovat všechny údaje uvedené v § 29 odst. 1 zákona č. 235/2004 Sb., o dani z přidané hodnoty, a dle zákona č. 563/1991 Sb., o účetnictví.
3. Splatnost faktury je 60 dní od doručení faktury nabyvateli do jeho sídla, Ekonomický úsek, Odbor účetnictví nebo elektronicky ve formátu PDF nebo ISDOC na e-mailovou adresu: faktury@vfn.cz.
4. Pokud faktura nebude obsahovat všechny zákonem a touto smlouvou stanovené náležitosti, je nabyvatel oprávněn ji do 15 dnů od doručení vrátit poskytovatel i s tím, že poskytovatel je poté povinen vystavit novou fakturu s novým termínem splatnosti. V takovém případě nabyvatel není v prodlení s úhradou faktury.
5. Faktury se platí bankovním převodem na účet druhé smluvní strany uvedený na faktuře. Povinnost nabyvatele zaplatit poskytovateli vyúčtovanou dohodnutou cenu je splněna dnem odeslání platby z účtu nabyvatele.
6. Cena za předmět plnění dle čl. IV. bude uhrazena po řádné akceptaci. Přílohou faktury bude akceptační protokol, který bude podepsán oběma smluvními stranami.
7. Nabyvatel se zavazuje zaplatit sjednanou cenu na základě faktury vystavené poskytovatelem do 14 dnů po řádném předání a převzetí předmětu plnění v celém jeho rozsahu dle podmínek uvedených v této smlouvě. Splatnost faktury činí 60 dnů od jejího doručení nabyvateli. Faktura může být zaslána elektronicky ve formátu PDF nebo ISDOC na e-mailovou adresu: faktury@vfn.cz nebo zaslána poštou ve dvou vyhotoveních na Ekonomický úsek nabyvatele, odbor účetnictví. K faktuře bude přiložena kopie řádně opatřeného akceptačního protokolu způsobem sjednaným níže. V případě zaslání faktury elektronicky bude akceptační protokol přiložen v neskenované podobě.
8. Poskytovatel se touto smlouvou zavazuje, že jím vystavená faktura bude obsahovat všechny náležitosti řádného daňového dokladu dle platné právní úpravy.
9. Platby budou probíhat výhradně v CZK.

### VI.

### Dodací podmínky

1. Poskytovatel bude informovat nabyvatele o termínu zahájení realizace předmětu plnění, a to nejméně 3 pracovní dny před zahájením realizace. Kontaktní osobou a odpovědným zaměstnancem nabyvatele je pro účely této smlouvy určen xxxKontaktní osobou poskytovatele je pro účely této smlouvy určen: Ivo Bolcek, xxx
2. Software bude nabyvateli poskytnut výhradně s využitím hardwarových prostředků nabyvatele.
3. Dodávka předmětu plnění se považuje podle této smlouvy za splněnou, pokud bylo provedeno následující:
* implementace do prostředí nabyvatele,
* byla provedena integrace se systémy nabyvatele, migrace dat a bylo provedeno nastavení SW řešení
* nabyvateli byly poskytovatelem předány licenční klíče, veškeré návody a doklady vztahující se k licencím, bezpečnostní dokumentace, uživatelské příručky, administrátorské dokumentace, provozní dokumentace a technické dokumentace popisující integrační vazby rozhraní.
* bylo provedeno zaškolení administrátorů a uživatelů nabyvatele
* byly úspěšně provedeny a nabyvatelem akceptovány testy uvedené v příloze č. 4 této smlouvy
* byla provedena finální akceptace předmětu plnění.
1. O řádném předání a převzetí předmětu plnění bude sepsán akceptační protokol, který podepíší obě smluvní strany. Nedílnou součástí předávacího protokolu jsou dílčí akceptační protokoly vztahující se k jednotlivým testům uvedeným v příloze č. 4 této smlouvy podepsané oběma stranami. Podpisem akceptačního protokolu o předání a převzetí předmětu plnění dochází k předání předmětu plnění poskytovatelem nabyvateli.
2. Nabyvatel není povinen akceptovat řádné předání a převzetí předmětu plnění v případě, že předmět plnění bude vykazovat vady a nedodělky. Pokud vada nebo nedodělek nebrání převzetí předmětu plnění smlouvy, musí být vždy uveden v akceptačním protokolu s uvedením data odstranění. Nebude-li nabyvatelem akceptováno řádné předání a převzetí předmětu plnění z důvodů vad a nedodělků, bude o této skutečnosti sepsán zápis s výčtem zjištěných vad nebo nedodělků, které zjistil nabyvatel, včetně způsobu a lhůt k jejich odstranění. Tento zápis bude současně podepsán zástupci obou smluvních stran.
3. Veškeré činnosti při aplikaci softwarového řešení je poskytovatel povinen provádět osobami, které mají odpovídající kvalifikaci.
4. Odpovědnou osobou nabyvatele oprávněnou podepsat předávací protokol je: xxx
5. Odpovědnou osobou poskytovatele oprávněnou podepsat předávací protokol je: Ivo Bolcek

**VII.**

**Podpora SW**

1. Po dobu užívání předmětu plnění nabyvatelem bude poskytovatel poskytovat nabyvateli rovněž podporu předmětu plnění. Podmínky poskytování podpory, údržby (maintenance) SW a služeb na vyžádání jsou upraveny v samostatné Smlouvě o poskytování služeb podpory software č. PO 5/S/22.

**VIII.**

**Sankční ustanovení**

1. Pro případ prodlení nabyvatele s úhradou sjednané ceny je poskytovatel oprávněn požadovat zaplacení smluvního úroku z prodlení ve výši 0,01 % z dlužné částky za každý den prodlení. Smluvní strany se dohodly, že poskytovatel je oprávněn požadovat zaplacení úroku z prodlení až po uplynutí 30 dnů od sjednané lhůty splatnosti.
2. V případě nedodržení termínu uvedeného v čl. II této smlouvy je nabyvatel oprávněn požadovat zaplacení smluvní pokuty ve výši 0,1% z celkové sjednané ceny bez DPH předmětu plnění za každý i započatý den prodlení s dodáním předmětu plnění. Nabyvatel je dále v těchto případech oprávněn odmítnout převzetí předmětu plnění a odstoupit od smlouvy.
3. V případě prodlení poskytovatele s dodržením termínů odstranění vad předmětu plnění, jsou-li uvedeny v akceptačním protokolu o předání a převzetí předmětu plnění, je nabyvatel oprávněn požadovat zaplacení smluvní pokuty ve výši 0,1 % z celkové ceny předmětu plnění bez DPH za každý i započatý den prodlení.
4. Za nedodržení některé z povinností stanovených v čl. XI odst. 1 a 2 této smlouvy má nabyvatel právo účtovat smluvní pokutu ve výši 10.000,- Kč.
5. V případě nedodržení povinností poskytovatele dle bodu 4 a 5 čl. I. a čl. IX. této smlouvy, má objednatel právo účtovat poskytovateli smluvní pokutu ve výši 200.000,- Kč za každé jednotlivé porušení povinnosti.
6. V případě nedodržení povinnosti stanovené v čl. XI. odst. 7 smlouvy má nabyvatel právo účtovat smluvní pokutu ve výši pohledávky, která byla postoupena v rozporu s touto smlouvou. Nabyvatel má zároveň právo odstoupit od smlouvy.
7. Úhrada smluvní pokuty nevylučuje nárok na náhradu škody. Tato náhrada škody se týká i prokazatelných finančních ztrát nabyvatele, způsobených prodlením poskytovatele s dodržením konečného termínu předání předmětu plnění, a tím způsobenou prodlevou v léčebných procesech.
8. Smluvní pokuta bude vyúčtována samostatným daňovým dokladem se splatností 30 dnů po obdržení vyúčtování této pokuty.

IX. Mlčenlivost

1. Poskytovatel se zavazuje zachovávat mlčenlivost ve vztahu ke všem informacím a skutečnostem, které se dozví o nabyvateli, jeho zaměstnancích, pacientech atd. v souvislosti s uzavřením a plněním smlouvy, pokud tyto informace mají povahu obchodního tajemství, osobních údajů nebo mají být z jiných důvodů chráněny před zveřejněním. Poskytovatel je povinen nakládat s osobními údaji a zejména s údaji o zdravotním stavu, genetickými a biometrickými údaji (dále jen „Osobní údaje“) v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 (dále jen GDPR) a příslušnými ustanoveními zákona č. 110/2019 Sb., o zpracování osobních údajů.
2. Povinnost mlčenlivosti platí rovněž o skutečnostech, na něž se vztahuje povinnost mlčenlivosti zdravotnických pracovníků, zejména podle ustanovení § 51 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (Zákon o zdravotních službách), a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení Osobních údajů.
3. Pokud poskytovatel přijde při plnění Smlouvy do styku s Osobními údaji a bude v postavení zpracovatele ve smyslu GDPR a Zákona o zpracování osobních údajů, zavazuje se nakládat s Osobními údaji pouze za účelem splnění závazků z této smlouvy a žádným jiným způsobem, a to v souladu příslušnými ustanoveními GDPR a Zákona o zpracování osobních údajů v rozsahu nezbytném pro plnění smlouvy a po dobu nezbytnou k plnění smlouvy. Zpracovávání Osobních údajů v rozsahu údajů poskytnutých nabyvatelem a týkajících se zdravotnické dokumentace pacientů, jimž jsou nabyvatelem poskytovány zdravotní služby, a dále v rozsahu Osobních údajů zaměstnanců nabyvatele poskytovatelem může zahrnovat odstranění potíží za účelem zabránění, vyhledávání a opravy problémů zjištěných při poskytování služeb dle této smlouvy, může také zahrnovat zlepšování funkcí informačních systémů, vyhledávání hrozeb uživatelům a ochrany uživatelů informačních systémů. Osobní údaje nebudou použity k jinému účelu, ani z nich nebudou odvozovány informace pro žádné reklamní či jiné komerční účely. Poskytovatel se zavazuje za účelem ochrany osobních údajů nabyvatele a jeho pacientů a zaměstnanců před neoprávněným přístupem, použitím, zveřejněním nebo zničením, resp. před jejich náhodnou ztrátou či změnou uplatňovat technická a organizační bezpečnostní opatření, interní kontroly a rutiny zabezpečení osobních údajů zajišťující splnění všech povinností dle GDPR a Zákona o zpracování osobních údajů, zejména zajistit, aby data obsažená ve zdravotnické dokumentaci byla šifrována způsobem, který znemožní nahlížení do těchto údajů neoprávněným osobám.
4. Poskytovatel se zavazuje zajistit informovanost svých pracovníků (včetně poddodavatelů) o povinnostech vyplývajících z této Smlouvy. Poskytovatel se zavazuje zajistit, aby jeho pracovníci, kteří budou přicházet do styku s osobními údaji, byli smluvně vázáni povinností mlčenlivosti ve smyslu GDPR a Zákona o zpracování osobních údajů a poučeni o možných následcích porušení těchto povinností s tím, že povinnost důvěrnosti bude jimi dodržována i po skončení jejich smluvního vztahu k nabyvateli. Toto ujednání je sjednáno ve smyslu ustanovení čl. 28 GDPR. Poskytovatel se zavazuje informovat své poddodavatele o povinnosti mlčenlivosti dle této smlouvy. V případě porušení mlčenlivosti za strany poddodavatele, odpovídá poskytovatel nabyvateli za vzniklou škodu, jako kdyby povinnost porušil sám.
5. Smluvní strany se zavazují zachovat mlčenlivost též o všech ostatních skutečnostech, ve vztahu k nimž o to budou druhou stranou písemně požádány. Smluvní strany se též zavazují nevyužít informace podle prvé věty tohoto odstavce ve svůj prospěch nebo ve prospěch třetích osob v rozporu s účelem jejich předání.
6. Smluvní strany jsou povinny zajistit, že nebudou neoprávněně pořizovány kopie informací či jiné záznamy nad rámec plnění dle této smlouvy, a nebudou zjišťovány informace, které nejsou nezbytně nutné ke splnění povinností vyplývajících z této smlouvy.
7. Smluvní strany se zavazují pro případ, že se v průběhu plnění dle této smlouvy dostanou do kontaktu s údaji druhé smluvní strany vyplývajícími z její provozní činnosti, tyto údaje v žádném případě nezneužít, nezměnit ani jinak nepoškodit, neztratit či neznehodnotit.
8. Poskytovatel se zavazuje plně respektovat bezpečnostní požadavky nabyvatele k zajištění ochrany Osobních údajů pacientů a zaměstnanců nabyvatele.
9. Povinnost mlčenlivosti o informacích a skutečnostech obchodního charakteru trvá po dobu 5 let od ukončení této smlouvy, o informacích obsahujících Osobní údaje trvá bez časového omezení.

**X.**

**Trvání licenční smlouvy, odstoupení od smlouvy**

Smlouva nabývá platnosti jejím uzavřením a účinnosti dnem uveřejnění v registru smluv.

Kterákoliv ze smluvních stran je oprávněna od této smlouvy odstoupit v případě jejího podstatného porušení druhou smluvní stranou. Pro účely této smlouvy se za podstatné porušení smluvních povinností považuje takové porušení, u kterého strana porušující smlouvu měla nebo mohla předpokládat, že při takovémto porušení smlouvy, s přihlédnutím ke všem okolnostem, by druhá smluvní strana neměla zájem smlouvu uzavřít, zejména:

* na straně poskytovatele, pokud dojde z jeho viny k posunu termínu předání předmětu plnění, přestože byl nabyvatelem na neplnění této smlouvy písemně upozorněn.
* na straně nabyvatele nezaplacení sjednané ceny předmětu plnění podle této smlouvy ve lhůtě delší 60 dní po dni splatnosti příslušné faktury, přestože byl poskytovatelem na neplnění této smlouvy písemně upozorněn.

Odstoupení od smlouvy musí být provedeno písemným oznámením o odstoupení, které musí obsahovat důvod odstoupení a musí být doručeno druhé smluvní straně. Účinky odstoupení nastanou okamžikem doručení písemného vyhotovení odstoupení druhé smluvní straně.

**XI.**

**Ostatní ujednání**

1. Poskytovatel se zavazuje, že bude mít po celou dobu plnění smlouvy řádně uzavřené pojištění odpovědnosti za škodu způsobenou třetí osobě ve výši minimálně 1 000 000 Kč. Na žádost nabyvatele je poskytovatel povinen kdykoli v průběhu trvání smlouvy předložit kopie aktuálních pojistných smluv.
2. Poskytovatel je povinen udržovat pojištění dle čl. XI. odst. 1 této smlouvy po celou dobu trvání této smlouvy. V případě porušení této povinnosti je nabyvatel oprávněn od této smlouvy odstoupit. Pokud by v důsledku pojistného plnění nebo jiné události mělo dojít k zániku pojištění, k omezení rozsahu pojištěných rizik, ke snížení stanovené min. výše pojistného plnění, nebo k jiným změnám, které by znamenaly zhoršení podmínek oproti původnímu stavu, je poskytovatel povinen učinit příslušná opatření tak, aby pojištění bylo udrženo tak, jak je požadováno v tomto ustanovení.
3. Obě strany se zavazují, že v souvislosti s plněním smlouvy učiní opatření k zajištění ochrany před šířením počítačových virů a nelegálních programů.
4. Poskytovatel prohlašuje, že poskytnutím licence k užívání software dle této smlouvy neporušuje práva třetích osob ve smyslu autorského práva a že tak činí v souladu s příslušnými ustanoveními občanského zákoníku.
5. Poskytovatel je povinen v souladu s ustanovením § 105 z. č. 134/2016 Sb. předložit do 10 pracovních dnů od doručení oznámení o výběru poskytovatele nabyvateli seznam, ve kterém uvede, jaké části předmětu plnění a v jakém rozsahu bude plnit prostřednictvím poddodavatele, spolu s identifikací poddodavatele a uvedením rozsahu jeho plnění, pokud mu jsou známi. Poddodavatelé, kteří nebyli tímto způsobem identifikováni a kteří se následně zapojí do plnění veřejné zakázky, musí být identifikováni dodatečně, a to nejpozději před zahájením plnění veřejné zakázky tímto poddodavatelem.
6. Poskytovatel bere na vědomí, že nabyvatel je povinen dle ustanovení § 219 odst. 1 zákona č. 134/2016 Sb., o zadávání veřejných zakázek a dle zákona č. 340/2015 Sb., o registru smluv, zveřejnit tuto smlouvu včetně případných dodatků zákonem stanoveným způsobem.
7. Poskytovatel je oprávněn postoupit pohledávku vyplývající z plnění dle této smlouvy na třetí osobu pouze s předchozím písemným souhlasem nabyvatele.
8. Poskytovatel se zavazuje dodržovat nařízení nabyvatele, kterým je zakázáno kouření ve všech prostorách i plochách areálu nabyvatele s výjimkou vyhrazených míst.
9. Poskytovatel se zavazuje při plnění této smlouvy dodržovat povinnosti uvedené v dokumentu „Používání sítě VFN externími uživateli“, který je přílohou č. 5 této smlouvy.

**XII.**

### Závěrečná ujednání

* 1. Tato smlouva nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti dnem uveřejnění v registru smluv.
	2. Tato smlouva se řídí právním řádem České republiky a případné spory z ní, které nebudou urovnány smírnou cestou, budou rozhodovány příslušným soudem. Právní vztahy touto smlouvou neupravené, jakož i právní poměry z ní vznikající a vyplývající, se řídí příslušnými občanského zákoníku v platném znění a předpisy souvisejícími.
	3. Jakékoliv změny této smlouvy mohou být prováděny pouze formou písemných číslovaných dodatků k této smlouvě a musí být podepsány oprávněnými zástupci smluvních stran. Tyto případné dodatky budou tvořit nedílnou součást této smlouvy.
	4. Tato smlouva je vyhotovena ve dvou stejnopisech, z nichž každá ze smluvních stran obdrží po jednom vyhotovení. Nedílnou součástí této smlouvy jsou přílohy dle textu smlouvy.
	5. Práva a závazky, které pro smluvní strany ze smlouvy vyplývají, přecházejí na jejich případné právní nástupce.
	6. Smluvní strany prohlašují, že si tuto smlouvu přečetly, a že byla ujednána po vzájemném projednání podle jejich svobodné vůle, určitě, vážně a srozumitelně, nikoliv v tísni za nápadně nevýhodných podmínek.

Přílohy:

Příloha č. 1 – Technická specifikace předmětu plnění nabídka

Příloha č. 2 – Položkový ceník

Příloha č. 3 – Minimální specifikace nezbytné součinnosti nabyvatele pro zpracování předimplementační analýzy

Příloha č. 4 – Testy ověření kvality dodávky

Příloha č. 5 – Používání sítě VFN externími uživateli

Příloha č. 6 – Požadavky na bezpečnost

V Praze dne V Ostravě dne

------------------------------------------------------------------ -----------------------------------------------------

Všeobecná fakultní nemocnice v Praze Za dodavatele

prof. MUDr. David Feltl, Ph.D., MBA, ředitel Ivo Bolcek

Příloha č. 1 smlouvy PO 4 /S/22

1. **Způsob zpracování a popis částí IS SW ZDS.**
	1. **Zpracování.**

Celý IS SW ZDS je zpracován modulárně a je sestaven tak, aby bylo možné jednoduchým způsobem organizovat různé zdravotnické převozy s následným vyúčtováním zdravotním pojišťovnám. IS SW ZDS lze datově propojit s externími systémy.

* + 1. **PKZT (Příkaz ke zdravotnímu transportu).**

PKZT je modul, který je nezávislý na použitém NIS a pomocí předaných parametrů z NIS kompletuje data pro vlastní zadání PKZT včetně předání na ZDS. V PKZT je hlavně kladený důraz na kontrolu povinných položek s možností doplnění uživatelských kontrol, které budou zajišťovat správnost této žádanky. Pro ZDS představuje tato žádanka v elektronické podobě velké usnadnění příjmu požadavků z jednotlivých klinik, a to tím, že se přenesou v elektronické podobě údaje o pacientovi jako je příjmení, jméno, číslo pojištěnce, diagnózy a další položky, zejména kompletní a správná adresa odkud a kam, dle strukturovaného celostátně platného místopisu včetně souřadnic. Tím je pro ZDS zajištěn nejen jednodušší způsob zadání požadavků pro organizaci převozů v modulu Dispečer, ale taktéž se přenesou údaje pro vykazování pojišťovnám a nebude docházet k chybovosti při vyúčtování v modulu Pojišťovny. Díky souřadnicím v místopisu, které využívá PKZT bude známá i vzdálenost odkud a kam. PKZT bude přínosem i pro jednotlivé kliniky, protože se v PKZT budou nabízet adresy odkud a kam u již vezených pacientů a sdílení některých hodnot jednotlivých položek s ZDS.

* + 1. **Dispečer.**

Tento SW modul umožňuje efektivně organizovat převozy (ZDS, JHČ), plánovat převozy, podporuje periodicky opakující se převozy, organizaci skupinek ve vazbě na posádku s další možností rozšiřování funkcionality dle konkrétních požadavků. Další podporou jsou různě nastavitelné filtry, dále pak možnost vkládat již vezené pacienty z registru vezených pacientů, plánování směn řidičů, samaritánů a dispečerů, volba jízdy zpět, zpětné zařazení pacientů do vezených a přijatých. Adresy míst, odkud a kam se pacienti vezou, jsou plně podporovány RÚIAN místopisem. Algoritmy pro použitý místopis umožňují z nekompletních adres dohledat zbývající části tak, aby bylo možno jednoznačně určit PSČ a zkomponovat adresu pro SW modul Pojišťovny (je obsaženo i v SW modulu Pojišťovny).

* + 1. **Pojišťovny.**

Tento SW modul je sestaven tak, aby bylo možné jednoduchým způsobem zadávat údaje o pacientech nebo používat údaje z modulu Dispečer s následným vyúčtováním zdravotním pojišťovnám. Číselníky z pojišťoven jsou importovány z textových souborů distribuovaných pojišťovnou. Při pořizování dat se údaje o pacientech zaznamenávají do registru pojištěnců pro možné další kontroly a zrychlení vkládání dat při opětovném použití. Systém je sestaven tak, aby mohl pružně reagovat na změny v metodice pojišťoven pro pořizování a předávání dokladů. Při pořizování dat se vytvářejí podklady pro statistiky. SW modul Pojišťovny je integrovaný s „T-MAPY“ pro zjištění vzdálenosti, vše probíhá v SW modulu Pojišťovny s automatickým přiřazením kódu s ohledem na doprovod, infekci a paušál).

* + 1. **SMS (Posílání informací o převozech do mobilu).**

Modul SMS umožňuje přenášet údaje o pacientech, kteří se mají převážet, do mobilu, který bude vázaný na auto nebo řidiče. Nastavit lze automatické nebo ruční odesílaní, odesílání na mobil řidiče nebo auta a taktéž selektivní odesílání. Do mobilu se přenášejí všechny potřebné údaje, které řidič potřebuje pro převoz pacientů. Modul SMS usnadňuje komunikaci mezi dispečerem a řidičem a řidič si nemusí zapisovat nebo pamatovat údaje pro převoz pacientů.

Pro přenos informací do mobilu je potřebný externí modem, který bychom vám doporučili.

* + 1. **Přehled modulových částí IS SW ZDS**
* interní číselníky – pracoviště, stanoviště, objekty, žadatelé, auta, osoby, nastavení směny, objekty, nákladová střediska …
* externí číselníky - diagnózy, dopravní výkony, odbornosti, …
* import žadatelů
* PKZT (Příkaz ke zdravotnímu transportu)
* SMS (Posílání informací o převozech do mobilu)
* organizace příjmu žádostí o převoz ZDS, JHČ
* organizace převozu přijatých žádostí pro ZDS, JHČ
* organizace uzavření žádostí pro ZDS, JHČ
* přehled zrušených převozů
* barevné rozlišení převozů
* objednané převozy
* možnost vytvářet skupinky pacientů pro převoz
* náhled na skupinku s možností nahlášení převozu
* generování jednoznačné výzvy pro každý den a převoz
* filtr pro organizaci převozu (typ převozu, stanoviště, místní převoz, dálkový převoz, datum převozu, mobilní a imobilní pacient, …)
* stálé převozy (periodicky opakující se převozy)
* plán směn řidičů, samaritánů a dispečerů
* směna řidičů, samaritánů a dispečerů
* možnost importu směn z jiných plánovacích systémů
* převod stálých převozů do operativní organizace převozů
* převod směny řidičů z plánu do směny
* nabídka opakujících se převozů dle jména pacienta
* jízda zpět
* zařazení pacienta zpět do vezených a do příjmu
* registr pacientů
* export a import registru pacientů (doplnění aktuální pojišťovny u pacientů)
* automatická změna pojišťovny u pacientů v záznamech z registru pacientů (s potvrzením)
* dodatečný přepočet hodnot výkonů
* uzavření záznamu s kontrolou
* volitelné generování dokladů
* přehled o verzích číselníků z pojišťoven
* přehled dávek
* validace vstupních dat
* opakovatelnost položek (datum, řidič, stanoviště, …)
* hromadná syntaktická kontrola dat za všechny pojišťovny, charaktery dávek a pracoviště za zvolené období (pro VZPKONTROL)
* interní kontrola záznamů (náhrada VZPKONTROL)
* nastavení předdefinovaných hodnot
* uzávěrka EU cizinců
* uzávěrka smluvních pojištěnců
* vyúčtování samoplátců
* vstup pro externí dávky
* statistiky
* tiskové výstupy
* exporty a importy dat
* exporty sestav do pdf, xls, doc a rtf
* autorizovaný přístup
* konfigurovatelnost
* filtry
* automatická a ruční záloha dat
* kompletní místopis ČR (RÚIAN)
* možnost propojení s „T-MAPY“
* přehled sil a prostředků
* historie směn
* vytíženost řidičů
* audit záznamů
* a mnoho dalších funkcí.
	1. **Možnosti.**

Prostředky IS SW ZDS umožňují nejen informace o pacientovi zaevidovat, ale také připravovat a udržovat v aktuálním stavu číselníky informační podpory. Informační podporou rozumíme veškerá data, která musí být nejprve do výpočetního systému vložena. Jsou předpokladem pro rychlý a bezchybný chod IS SW ZDS. Sem patří základní informace o pojišťovnách, diagnózách, řidičích, autech, atd. Základními kritérii důsledně uplatňovanými při vývoji IS SW ZDS jsou vysoká rychlost odezvy, maximální spolehlivost a bezpečnost při dodržení vysoké kvality uživatelského rozhraní (komplexnost funkcí, jednoduchost a srozumitelnost ovládání). Vše, co je možné vykonat automaticky, bude se dělat skutečně automaticky, ovšem i zde bude hlavním kritériem bezpečnost prováděných akcí, ale i velká informovanost uživatele. Manipulace s daty je velmi jednoduchá a přehledná. Data se zobrazují pomocí různých formulářů, které jsou navrženy tak, aby měl uživatel co nejlepší přehled o všem, co potřebuje. Pro každou skupinu dat je k dispozici aktualizační formulář, který zobrazuje veškeré detailní informace, a ve kterém je uživatel oprávněn s daty manipulovat, tabulkový formulář nabízející přehled o všech uložených datech přehlednou tabulkovou formou a výběrový formulář, kde lze na základě určitých kritérií provádět různé výběry. Data je možno si kdykoliv setřídit podle libovolných položek. IS SW ZDS je otevřený pro komunikaci s programy třetích firem.

* 1. **Režim.**

IS SW ZDS pracuje v režimu klient-server a zabezpečení přístupu k datům probíhá kontrolou hesla uživatelů hlásících se do systému. IS SW ZDS využívá databázový systém SQL Server.

Příloha č. 2 smlouvy PO 4 /S/22

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Položka** | **Název**  | **Položka** | **MJ** | **ks** | **Jednotková cena bez DPH (Kč)** | **Celková cena bez DPH (Kč)** |
| č. 1 | Modernizace dispečinku zdravotní dopravní služby | Časově neomezená užívací práva k SW řešení pro organizaci provozu sanitní dopravy včetně: zpracování předimplementační analýzy, Implementace SW řešení do technologického prostředí zadavatele, Integrace se systémy zadavatele, migrace dat a nastavení SW řešení, zpracování dokumentace a provedení školení administrátorů a uživatelů zadavatele. | multilicence | 1 |  790 000,00  |  790 000,00 |

**Příloha č. 3 smlouvy PO 4/S/22**

1. Poskytovatel se zavazuje zahájit předimplementační analýzu a zpracování navazujícího implementačního projektu bezodkladně poté, co tato smlouva nabyde účinnosti, k čemuž mu objednatel poskytne veškerou nezbytnou součinnost, kterou lze na něm důvodně požadovat.
2. V průběhu předimplementační analýzy, instalace a integrace IS se účastníci zavazují poskytovat si součinnost formou konzultací obou stran takto:
	1. Obsahem konzultací je zjišťování, upřesňování a konkretizace požadavků nabyvatele na IS a podmínek pro jeho realizaci, včetně postoupení příslušných vnitřních předpisů nabyvatele, které se vztahují k plnění této smlouvy.
	2. Smluvní strany jsou povinny neprodleně si vzájemně sdělovat informace, které mohou mít vliv na plnění závazků vyplývajících z této smlouvy.
	3. Veškerá komunikace mezi smluvními stranami bude probíhat v českém jazyce a prostřednictvím osob, které jednotlivé smluvní strany určí.
	4. Obě smluvní strany jsou povinny účastnit se předem dohodnutých konzultací. Sjednává se, že o průběhu konzultací bude poskytovatel pořizovat písemné záznamy obsahující vyjádření obou stran.
	5. Nabyvatel je povinen zabezpečit informovanost svých zaměstnanců o probíhající předimplementační analýze, implementaci IS a oprávnění poskytovatele požadovat konzultace.
3. Nabyvatel je povinen zabezpečit součinnost dodavatelů systémů třetích stran (Webdispečink, NIS, …), jejichž integrace a komunikace s IS se vztahují k plnění této smlouvy. Jestliže nabyvatel nezajistí dostatečnou součinnost třetích stran, případně nedodá informace podstatné pro další postup poskytovatele při předimplementační analýze v předem dohodnutý termín, posouvá se termín plnění o dvojnásobek dnů prodlení nabyvatele.
4. Jestliže nabyvatel neposkytne poskytovateli součinnost účastí na předem dohodnuté konzultaci, případně nedodáním informace podstatné pro další postup poskytovatele při předimplementační analýze a instalaci IS, posouvá se termín plnění o dvojnásobek dnů prodlení nabyvatele.
5. V případě, že některá ze smluvních stran bude mít za to, že ji druhá strana neposkytuje dostatečnou součinnost dle ujednání této smlouvy, je povinná písemně na tuto skutečnost upozornit druhou smluvní stranu a současně ji písemně vyzvat k nápravě. V případě, že smluvní strana písemně neupozorní druhou smluvní stranu na nedostatečné poskytování součinnosti a současně ji písemně nevyzve k nápravě, pak platí, že druhá smluvní strana poskytovala řádně a dostatečně součinnost dle ujednání této smlouvy.

Příloha č. 4 smlouvy PO 4/S/22

**Testy ověření kvality dodávky**

### Funkční test

Poskytovatel se zavazuje ověřit kvalitu všech dodávek před jejich předáním nabyvateli provedením funkčního testu (FAT), který bude zaměřen na dodržení souladu s metodikou vedení implementačního projektu, se standardy vývoje SW a poskytování služeb údržby SW, s obecně závaznými právními předpisy, a to nejméně v tomto rozsahu:

1. Testování funkčnosti nových a modifikovaných modulů,
2. Ověření funkčnosti těchto modulů v kontextu návazných aplikačních procesů,
3. Integrační testy – ověření funkčnosti komunikace s externími systémy.
4. Ověření instalační sady včetně kontroly správnosti a úplnosti sestavení dodávky,
5. Ověření dodržení bezpečnostních standardů použitých pro webové služby a SW aplikace.
6. Ověření dodržení požadavků nabyvatele na výkonnost systému a minimální dobu odezvy.

Výstupem funkčního testu je předání řešení poskytovatelem do uživatelského akceptačního testu nabyvateli s následujícími předměty dodání:

1. Protokol o provedení funkčního testu a jeho výsledky v elektronické podobě,
2. Testovací scénáře pro provedení uživatelského akceptačního testu.

### Systémový integrační test

Systémový integrační test (SIT) provádí nabyvatel za podpory poskytovatele. Tento test se provádí v testovacím prostředí nabyvatele.

1. Cílem testů je ověřit funkčnosti celého systému jako celku, včetně komunikace s okolními systémy.
2. Součástí testování je správná komunikace jednotlivých komponent uvnitř aplikace.
3. Systémové integrační testy jsou prováděny na základě testovacích scénářů poskytovatele,
4. Všechny chyby zaznamenané v průběhu SIT budou dokumentovány, kategorizovány podle jejich závažnosti a předány poskytovateli k řešení,
5. Opravy chyb budou jednoznačným a pro nabyvatele dostupným způsobem evidovány a dokumentovány, např. samostatnými položkami v helpdesku nabyvatele,
6. Podmínky úspěšného ukončení SIT jsou stanoveny v předimplementační analýze.

Výstupem SIT je report a akceptační protokol.

###

### Penetrační testy

Dodávané řešení musí podléhat nezávislému bezpečnostnímu testování (penetrační testy). Rozsah testů bude zaměřen na infrastrukturu a aplikační vrstvu. Tyto testy budou provedeny zadavatelem (prostřednictvím 3. strany) a zjištěné zranitelnosti musí být dodavatelem odstraněny před akceptací dodávaného řešení. V průběhu akceptace řešení bude ověřeno odstranění zranitelností retesty zadavatelem.

###

### Uživatelský akceptační test

Uživatelský akceptační test (UAT) provádí nabyvatel za podpory poskytovatele. Tento test se provádí v testovacím prostředí nabyvatele.

1. Uživatelský akceptační test je prováděn na základě testovacích scénářů dodaných poskytovatelem po provedení funkčního testu,
2. Všechny chyby zaznamenané v průběhu UAT budou dokumentovány, kategorizovány podle jejich závažnosti a předány poskytovateli k řešení,
3. Opravy chyb budou jednoznačným a pro nabyvatele dostupným způsobem evidovány a dokumentovány, např. samostatnými položkami v helpdesku nabyvatele,
4. Poskytovatel dodá opravenou (aktualizovanou) dokumentaci dle specifikací uvedených v bodě 1e) čl. I. této smlouvy po zapracování chyb a oprav z UAT testů,
5. Poskytovatel umožní nabyvateli ověřit řešení/modifikaci pilotním provozem na vybraných pracovištích či si k uživatelskému akceptačnímu testu přizvat externího konzultanta.
6. Podmínky úspěšného ukončení UAT jsou stanoveny v předimplementační analýze,
7. Součástí UAT v průběhu implementačního projektu bude zátěžový test, který ověří dodržení požadavků nabyvatele na výkonnost systému a minimální dobu odezvy.

Výstupem UAT je akceptační protokol, který odpovídá podmínkám stanoveným v předimplementační analýze.

Příloha č. 5 smlouvy PO 4 /S/22

xxx

Příloha č. 6 smlouvy PO 4/S/22

Příloha č. 6 – Požadavky na bezpečnost

**Požadavky na bezpečnost řešení**

Dodávané řešení musí být navržené, vyvíjené, konfigurované, implementované, nastavené, testované a zdokumentované a provozované v souladu s požadavky, specifikacemi a zásadami definované v mezinárodní normě ISO/IEC 27001:2013 (resp. 2014), ISO 27799:2016 (doporučení a požadavky na řízení bezpečnosti informací ve zdravotnických zařízeních), NIST SP 800 řady, metodice OWASP a v souladu s příslušnou legislativou vztahující se na celý předmět dodávky (zejména nařízením EU č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR) a zákona č. 110/2019 Sb., o zpracování osobních údajů) a to vše v níže uvedeném rozsahu (kap. 1) až 12)).

## 1) Požadavky kybernetické bezpečnosti

## Dodávané řešení z pohledu kybernetické bezpečnosti musí splňovat nebo zajistit:

## Dodávané technické nebo programové prostředky nesmí být prostředky, které jsou zveřejněny na stránkách Národního centra kybernetické bezpečnosti (provozované NÚKIB) jako hrozba. Veškeré poskytované služby nesmí být provozované na technických nebo programových prostředcích označených NÚKIB jako hrozba.

## Při implementaci nebo zajištění podpory dodávaného řešení musí být zajištěno neprodlené informování zadavatele prostřednictvím dodavatelem určené odpovědné osoby: Manažera kybernetické bezpečnosti, o kybernetických bezpečnostních incidentech.

## 2) Analýza rizik navrhovaného řešení

Poskytovatel musí provést v rámci předimplementační analýzy analýzu rizik navrhovaného řešení. Zejména pro technické vybavení, komunikační prostředky, programové vybavení, zpracování dat, datová nebo cloudová úložiště a objekty dodávaného řešení se zaměřením na následující hrozby:

1. poškození nebo selhání hardwaru nebo softwaru,
2. užívání software v rozporu s licenčními podmínkami,
3. škodlivý kód (např. viry, spyware, trojské koně),
4. přerušení dodávky komunikačních služeb nebo elektrické energie,
5. zneužití nebo modifikace údajů,
6. zneužití nebo prolomení přístupových oprávnění,
7. kybernetický útok z vnitřní sítě, zneužití vnitřních prostředků,
8. neposkytnutí garantovaných služeb (SLA),
9. selhání nebo nefungování kontrolních mechanismů nebo bezpečnostních funkcí,
10. zajištění kontinuity provozu,
11. fyzická bezpečnost.

Poskytovatel zpracuje na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti, které obsahuje přehled vybraných a zavedených bezpečnostních opatření a popis vazeb mezi identifikovanými riziky a příslušnými bezpečnostními opatřeními. Součástí bude i úroveň pokrytí rizika (např. %) navrženými opatřeními a možné dopady těchto zbytkových rizik.

## 3) Dokumentace

Poskytovatel musí v rámci předmětu plnění smlouvy zpracovat dokumentaci, která musí zahrnovat tyto provozní postupy, bezpečnostní specifikace a skutečnosti:

* 1. spuštění a ukončení chodu systému,
	2. instalace a konfigurace systému,
	3. bezpečnostní dokumentaci:
		1. bezpečnostní architektura,
		2. implementované kontrolní mechanismy a bezpečnostní funkce,
		3. privilegované a technické účty, privilegované role, matice rolí a neslučitelnost rolí,
		4. bezpečnostní logy v návaznosti na požadavky uvedené v kap. 8) a 9),
		5. řízení přístupu,
		6. bezpečnostní nastavení ochrany DB a dat,
		7. komunikační bezpečnost,
		8. použité kryptografické nástroje, funkce a klíče,
		9. verzování, kampaně, integrace, nezaměnitelnost apod.,
		10. popis datových rozhraní pro napojení na systémy 3. stran,
	4. monitoring provozu systémů, aplikací a služeb,
	5. administrátorská a uživatelská dokumentace,
	6. zpracování a nakládání s informacemi,
	7. vzájemné vztahy a vazby na jiné systémy,
	8. postupy zálohování a obnova systému a dat ze záloh,
	9. restart nebo obnovení chodu systému po selhání, ošetření chybových stavů anebo mimořádných jevů,
	10. podpora a eskalační kontakty v případě neočekávaných provozních nebo technických obtíží či bezpečnostních incidentů.

## 4) Požadavky na vývoj, test a provoz dodávaného řešení

1. Poskytovatel musí zajistit z pohledu zajištění bezpečnosti prostředí:
	1. Vývojové, integrační, testovací a provozní prostředí musí být zcela oddělena v sítích a musí být podporována oddělenými stroji.
	2. Provozní servery nesmí obsahovat překladače a systémové utility, které nejsou nezbytné pro jejich správu nebo provoz.
	3. Testování a vývoj nových verzí systémů, aplikací i zařízení se nesmí provádět v provozním prostředí.
2. Poskytovatel musí dodržovat při vývoji svých produktů zásady SDL (Secure Development Lifecycle).
3. Poskytovatel musí vydefinovat v rámci předimplementační analýzy požadavky na konfiguraci jednotlivých síťových a serverových prvků pro zajištění požadované bezpečnosti a funkčnosti.
4. Pro potřebu školení uživatelů na nový informační systém a testování nově nasazovaných verzí informačních systémů musí poskytovatel vytvořit testovací prostředí v dostatečném předstihu před pilotním provozem – duplicitní provoz.
5. poskytovatel musí zajistit úvodní migraci dat i potřebné služby pro testování informačních systémů. Poskytovatel musí testovací prostředí naplnit daty tak, aby bylo možné systém řádně otestovat. V rámci instalace nových verzí informačního systému bude zajištěna možnost pravidelně upgradovat provozovaná data a aplikace.
6. Řešení musí zahrnovat systém logování, které musí zahrnovat logy transakční a aplikační. V rámci systému pro logování musí být zajištěno:
	1. Správně nastavené časové značky na všech zdrojích (tj. synchronizovaný čas, jeho jednotný formát).
	2. Vydefinování dostatečné kapacity pro logování a jejich uchovávání po určenou dobu.
	3. Zajištění bezpečnosti a integrity log záznamů (ochrana před zneužitím, změněním nebo vymazáním) dle možné závažnosti zneužití.
	4. Dostupnost logů i v případě poruchy systému (zálohování).
	5. Umožnění pravidelného odesílání logů do centrálního log managementu nabyvatele.
7. Řešení musí umožňovat zálohování dat na základě specifikovaných zálohovacích plánů. Zálohovací plány předpisují, jak ochránit řešení a data při neočekávané události, tj. pádem systému počínaje a fyzickým zničením zařízení konče. Zálohovací plán řeší, jaká data, jakým způsobem a jak často se mají zálohovat, aby byly splněny požadavky uživatelů na:
	1. přijatelnou lhůtu obnovení dat ze zálohy,
	2. přípustný objem dat, který nebude možno obnovit (data od poslední zálohy),
	3. dobu omezení provozu IT z důvodu zálohování (zálohovací okno),
8. Zálohovací plán musí obsahovat:
	1. způsob zálohování (technologie, metoda),
	2. stanovení četnosti a cyklů záloh pro technologie, systémy a data,
	3. návrhy termínů zálohování (zálohovací okna),
	4. pravidla pro manipulaci s médii (bezpečnost uložení, skartace),
	5. stanovení Recovery Time Objective (RTO; jak rychle je možno data obnovit),
	6. stanovení Recovery Point Objective (RPO; jak staré mohou být zálohy),
	7. způsob testování záloh (ověření obnovitelnosti a čitelnosti).
9. Plány obnovy provozu řešení po rozsáhlém výpadku musí být zpracovány pro nejpravděpodobnější havárie s největším dopadem na činnost nabyvatele tak, aby snížily na minimum dobu zásahu, chybovost a riziko ze zanedbání důležitých souvislostí. Plány obnovy musí obsahovat:
	1. požadované instalační zdroje a nezbytné zálohy,
	2. pořadí a způsob obnovy jednotlivých komponent systémů,
	3. způsob ověření úspěšného obnovení dat ze zálohy,
	4. maximální časy potřebné na obnovu,
	5. kontaktní údaje servisních organizací,
	6. způsob testování plánů obnovy.

## 5) Postup ověření identity uživatelů a řízení přístupových oprávnění

1. Nabyvatel požaduje ověření identity (autentizace) v systému prostřednictvím ověření v LDAP (AD/AAD).
2. Z pohledu autentizace požaduje nabyvatel využití claim-based mechanismů. Identitním providerem a nastavení identitního systému bude včetně podpory Single Sign On s on-premise prostředím Active Directory. Nastavení pravidel pro hesla a podmíněné přístupy (vícefaktorové ověřování, komplexita hesla apod.) poskytuje nabyvatel. Nabyvatel preferuje použití protokolu Open ID Connect, alternativně je možné využít WS-Federation nebo SAML.
3. Z pohledu autorizace musí řešení podporovat hierarchizovatelné nastavení přístupových práv se stanovením rozsahu přístupu i stupně oprávnění manipulace se záznamem. Princip nastavování přístupových práv k jednotlivým uživatelům musí vycházet z definice libovolného množství uživatelských rolí a skupin, do kterých jsou jednotliví uživatelé přiřazováni v rámci identitního systému nabyvatele. Členství ve skupinách může systém kontrolovat v rámci claim informace v průběhu přihlašování protokolem Open ID Connect nebo alternativně vyžádat uživatelský token pro přístup na Graph API Active Directory pro vyčítání autorizačních informací.
4. Poskytovatel musí do dokumentace uvést detailní popis úrovně privilegovaných i neprivilegovaných přístupových oprávnění, resp. jednotlivých uživatelských rolí.

## 6) Ochrana před škodlivým kódem

V rámci dodávaného řešení musí být zajištěna a popsána ochrana:

1. komunikace ve vnitřní sítí,
2. ochrana serverů a sdílených datových úložišť,
3. popis požadavků na zajištění bezpečnosti pracovních stanic (HW klientů, popř. VDI).

## 7) Ověření zranitelnosti celého řešení

Součástí vývoje jsou i bezpečnostní testy a proces kontroly kódu (codereview), jejichž cílem je odhalit chyby a zranitelnosti dříve, než je aplikace schválena do provozu. Součástí implementačního procesu a průběžné podpory bude v několika krocích (beta testy, integrace, systémové testy a akceptační testy) provedení penetračních testů celého řešení, a to včetně příslušných testů aplikační vrstvy (např. testy xss, sql injection, rfi, lfi, code upload nebo OWASP top 10). Součástí akceptace bude provedení penetračních testů v souladu s normami ČSN ISO/IEC TR 13335 a ISO/IEC 27002:2013 dle obecně uznávané metodiky (např. OSSTMM, OWASP, NIST apod.).

## 8) Požadavky na logovací aparát

Všechny logovací aparáty musí obsahovat dle relevance minimálně tyto údaje:

* OS/DB/aplikace,
* druh záznamu/transakce/operace,
* u nových, změn nebo odstranění i zadanou/změněnou hodnotu,
* stav záznamu (dokončený/nedokončený/selhání),
* uživatel,
* datum a čas,

pro následující operace logování v systému (viz kap. 9)).

## 9) Zaznamenávání událostí a jejich vyhodnocování

V rámci dodávaného díla musí být realizováno zaznamenání minimálně následujících událostí:

1. přihlášení a odhlášení uživatelů a administrátorů,
2. činnosti provedené privilegovanými účty (administrátorské účty, systémové účty, technické účty apod.),
3. činnosti vedoucí ke změně přístupových oprávnění (standardních i privilegovaných),
4. neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů,
5. zahájení a ukončení činností (včetně „pádů“ nebo selhání) jednotlivých komponent systému,
6. činnosti spojené s přijímáním/odesíláním ze/do SW třetích stran (integrační logy),
7. automatická varovná nebo chybová hlášení komponent systému,
8. přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností,
9. použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení,
10. založení, změna, výmaz, čtení a tisk datových záznamu včetně času, uživatele a identifikace pracovní stanice, ze které byl úkon proveden (transakční protokol),
11. tracking systémových změn na úrovni operačního systému, služeb a aplikací,
12. identifikace pokusu nebo realizovaného kybernetického útoku.

Takto zaznamenané události musí být zpracovatelné (strukturované, strojově čitelné) nezávislým prostředkem pro ochranu získaných informací před neoprávněným čtením nebo změnou a pro další vyhodnocování (standardní rozhraní SIEM).

## 10) Aplikační bezpečnost

Poskytovatel zajistí v rámci dodávaného řešení:

1. trvalou ochranu aplikací a informací před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou,
2. trvalou ochranu transakcí před jejich nedokončením, nesprávným směrováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním.

## 11) Ochrana dat

Poskytovatel zajistí v rámci dodávaného řešení:

1. Nastavení ochrany dat zpracovaných nebo uchovávaných v řešení, a to především osobních údajů nebo citlivých údajů, kdy bude kladen důraz na data dostupná z vnější sítě. Budou zohledněna rizika:
	1. neoprávněného přístupu,
	2. nedovolených činností nad rámec svých práv,
	3. popření provedených činností,
	4. kompromitace,
	5. porušení integrity dat,
	6. nedostupnosti dat,
	7. neautorizované změny.
2. Ochranu prováděných transakcí nebo změn dat:
	1. před jejich nedokončením,
	2. nesprávným směrováním,
	3. neautorizovanou změnou předávaného datového obsahu,
	4. kompromitací,
	5. neautorizovaným duplikováním nebo opakováním, a to v souladu s legislativními nebo normativními požadavky, např. daňové, účetní, na ochranu dat.

## 12) Kryptografické prostředky

V případě využití kryptografických prostředků pro činnost dodávaného díla, poskytovatel zajistí použití kryptografických algoritmů a kryptografických klíčů v úrovni odolnosti vyplývající z analýzy rizik. Kryptografické klíče musí být uloženy v bezpečném prostředí s možností auditu přístupu ke klíčům.

Pro bezpečné uložení klíčů je možné využít službu Key Vault ve verzi Premium (založeno na HSM).

## 13) Zabezpečení síťových služeb

Realizace a dokumentace způsobu zabezpečení síťových služeb.

Virtuální servery v prostředí nabyvatele budou umístěny ve Virtuální síti, která bude propojena s on-premises datovým centrem nabyvatele. Hybridní propojení zajistí nabyvatel. Komunikace mezi jednotlivými funkčními celky bude řízená na úrovni síťových služeb a protokolů s pomocí network security groups. Povolena bude pouze vzájemná komunikace, která je nezbytná pro funkci systému.

Vstupní, výstupní i vzájemná síťová komunikace mezi jednotlivými částmi systému bude monitorována.