

# SMLOUVA O DÍLO

(dále jen „smlouva“)

*uzavřená ve smyslu ust. § 2586 a násl. a ust. § 1746 zákona č. 89/2012 Sb., občanského zákoníku (dále jen „Občanský zákoník“), ve znění pozdějších předpisů a podle zákona č. 121/2000 Sb. (dále jen „autorský zákon“), ve znění pozdějších předpisů*

## **Objednatel:**

### **Nemocnice Kadaň s.r.o.**

se sídlem: Golovinova 1559, 432 01 Kadaň  
IČ: 25479300  
ID datové schránky: z28pu9r  
jednatel: MUDr. Bc. Petr Hossner, MBA, jednatel  
bankovní spojení: UniCredit Bank Czech Republic and Slovakia, a.s.  
číslo účtu: 155977/2700

## **Zhotovitel nebo Účastník:**

### **STAPRO s. r. o.**

se sídlem: Pernštýnské náměstí 51, 530 02 Pardubice  
IČ: 13583531  
DIČ: CZ699004728  
za níž jedná: Ing. Leoš Raibr, jednatel společnosti STAPRO s. r. o.  
zapsaná v Obchodním rejstříku vedeném Krajským soudem v Hradci Králové spisová značka C 148  
tel.: +420 467 003 111 fax.: +420 467 003 119, e-mail: obchod@stapro.cz  
bankovní spojení: ČSOB a.s. / Oberbank AG  
číslo účtu: 271810793/0300 / 2171133923/8040  
dále společně jako „smluvní strany“

## **1. Preambule**

1.1. Objednatel uzavírá Smlouvu za účelem realizace zakázky spočívající v dodání software pro projekt s názvem „Transakční portál pro sdílení a výměnu dat včetně napojení na eHealth systém kraje a auditních služeb a podpory“. Objednatel má zájem na vytvoření, dodání a implementaci software transakční portál pro sdílení a výměnu dat včetně napojení na eHealth systém kraje a auditních služeb a podpory (dále jen „veřejná zakázka“).

## **2. Předmět smlouvy**

2.1. Předmětem smlouvy je závazek zhotovitele provést pro objednatele dílo spočívající v dodávce a implementaci portálového řešení, které bude napojené na interní provozní systémy (NIS, LIS, PACS, DocReg) a dohledové systémy (LOG management...) (dále také „Portál“) do prostředí objednatele, a to včetně nedílně souvisejících požadavků typu zaškolení, dodání licencí, dodání hardware, zpracování dokumentace v rozsahu dle zadávací dokumentace veřejné zakázky, nabídky zhotovitele a přílohy č. 1 této smlouvy. Dodávka bude zahrnovat zejména:

- Detailní analýza dodávky a nasazení Portálu.

- Dodávka licencí, implementace Portálu, jeho příslušenství, testovací provoz a předání do řádného užívání.
- Provedení integrací na další systémy v prostředí objednatele i mimo něj.
- Úpravy dodaného řešení dle potřeb a požadavků dle pokynů objednatele.
- Zaškolení odborného personálu (administrátorů a správců) objednatele.
- Příslušenství uvedené Příloze č 1.
- Hardware pro provoz dodaného řešení Portálu.
- Dokumentaci k dodanému plnění v požadovaném rozsahu.
- Další licence nezbytné pro provoz Portálu.
- Listinné potvrzení dodaných licencí co do jejich počtu a rozsahu.

Podrobná specifikace technického řešení díla je uvedena v Příloze č 1: Specifikace technického řešení této smlouvy a tvoří její nedílnou součást.

- 2.2. Předmět smlouvy rovněž obsahuje plnění, které není uvedeno v příloze č. 1 této smlouvy – Specifikaci technického řešení, ale jehož realizace je nezbytná pro provedení díla, tj. pro řádné a včasné dokončení díla v souladu s touto smlouvou. Zahrnuje veškerá plnění včetně software pro zajištění 100% funkčnosti a provozuschopnosti Portálu a dalších komponent na základě této smlouvy o dílo.
- 2.3. Vzdálený přístup: Předmětem této smlouvy je dále i zajištění a sjednání podmínek vzdáleného přístupu zhotovitele bez aktivní účasti objednatele do prostředí objednatele za účelem plnění této smlouvy. Objednatel se zavazuje, že umožní zhotoviteli potřebné vzdálené přístupy k informačním systémům a aplikacím uvedeným v předmětu plnění této smlouvy nejpozději do 10 pracovních dnů ode dne nabytí účinnosti této smlouvy.
- 2.4. Zhotovitel se zavazuje provést na svůj náklad a na své nebezpečí všechna související plnění a práce potřebné k včasnému a řádnému provedení díla.
- 2.5. Součástí smlouvy je i převod neomezeného vlastnického práva k tomuto dílu na objednatele. Součástí závazku zhotovitele je rovněž doprava zboží objednateli do místa plnění, jeho instalace a zprovoznění podle pokynů objednatele, a dále provádění záručních oprav díla.
- 2.6. U SW licencí je součástí smlouvy převod nevýhradních a nepřenositelných práv k užívání příslušné SW licence. Součástí závazku zhotovitele je rovněž doprava zboží objednateli do místa plnění včetně možnosti zpřístupnění el. licenčního klíče, jeho instalace a zprovoznění podle pokynů objednatele, a dále provádění záručních oprav díla.
- 2.7. Objednatel se zavazuje dílo řádně a včas dodané zhotovitelem převzít a zaplatit za něj sjednanou kupní cenu způsobem a v termínu sjednaném touto smlouvou.
- 2.8. Práce nad rozsah díla dle této smlouvy (vícepráce) budou realizovány jen pokud o ně bude po vzájemné dohodě písemným dodatkem k této smlouvě dílo rozšířeno.

### **3. Doba a místo plnění**

- 3.1. Zhotovitel se zavazuje, že dílo dodá objednateli nejpozději do 24 kalendářních týdnů od nabytí účinnosti této smlouvy. Zhotoviteli bude umožněn přístup do místa plnění.
- 3.2. Místem plnění je dle této smlouvy sídlo objednatele a další provozovny objednatele dle specifikace uvedené v zadávací dokumentaci veřejné zakázky.
- 3.3. Detailní závazný harmonogram plnění včetně dílčích milníků, na jejichž splnění v daném pořadí a čase objednatel bude trvat, je obsažen v příloze č. 3 této smlouvy o dílo – Závazný harmonogram plnění.

#### **4. Provedení a předání díla**

- 4.1. Provedením díla se rozumí úplné dodání dokončeného díla bez vad a nedodělků a současně řádné protokolární předání díla objednateli. Pro ověření plné funkčnosti díla bude po dobu 4 kalendářních týdnů probíhat testovací provoz v průběhu kterého budou provedeny akceptační testy. Smluvní strany tímto, po vzájemné dohodě, vylučují § 2628 Občanského zákoníku.
- 4.2. Součástí akceptačních testů musí být minimálně ověření (otestování) veškerých požadovaných funkcí a parametrů všech dodávaných komodit, funkcionalit uvedených v Příloze č. 1. O provedení akceptace a jejím výsledku musí být vyhotoven písemný protokol.
- 4.3. Podkladem k akceptaci dodávaného řešení je potvrzený výsledek akceptačního testu funkcionality za jednotlivé části Portálu, provedeného v závěru testovacího provozu a přehled zapracování připomínek klasifikace Incident/Vada všech kategorií.
- 4.4. Přejímací řízení do ostrého provozu se rozumí okamžik úspěšné akceptace díla (výsledek souhrnného akceptačního řízení) včetně vypořádání všech vad a nedodělků.
- 4.5. Výsledkem souhrnného akceptačního řízení bude akceptační protokol s výsledkem Splněno / Splněno s výhradou / Nesplněno, podepsaný oprávněnými osobami smluvních stran. Klasifikace Splněno s výhradou umožní akceptaci díla v případě vad drobných, pro které může být opakování akceptačního řízení zbytečně nákladné. Vadou se pro účely této smlouvy dále rozumí odchylka v kvantitě, kvalitě, rozsahu, termínech nebo parametrech díla stanovených touto smlouvou, zadávací dokumentací a obecně závaznými předpisy.
- 4.6. Předání dílčích plnění se uskuteční fyzickým převzetím (u SW podpory předáním přístupových hesel a uživatelských manuálů, u dokumentace předáním papírové / elektronické verze příslušné dokumentace, u školení provedením příslušného školení) objednatelem. Předání díla bude oboustranně stvrzeno podpisem předávacího protokolu. Předávací protokol bude podepsán oprávněnými zástupci obou smluvních stran. Dílo se považuje za převzaté a předané okamžikem podpisu předávacího protokolu, v němž objednatel prohlásí, že dílo přijímá.
- 4.7. Předávací protokol musí obsahovat předmět a charakteristiku předmětu díla, jakož i prohlášení objednatele dle § 2605 Občanského zákoníku, že dílo přijímá předvedením jeho způsobilost sloužit svému účelu. Předávací protokol bude vyhotoven ve třech stejnopisech, z nichž jeden obdrží zhotovitel a dva objednatel. Každý stejnopis bude podepsán oběma stranami a má právní sílu originálu.
- 4.8. Veškerá dokumentace projektu bude zhotovitelem objednateli předávána v originálech, a to jak ve formě listinných dokumentů, tak v elektronické editovatelné podobě. Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána ve 2 kopiích v elektronické formě ve standardních formátech (např. MS Office (.docx) nebo PDF) používaných zadavatelem na datovém nosiči a 1x v kopii v papírové formě. Předána bude implementační analýza, uživatelská dokumentace, administrátorská a bezpečnostní dokumentace, popis integračních vazeb a případná další dokumentace v rozsahu odpovídajícím předmětu díla dle této smlouvy.
- 4.9. Nejpozději na poslední den provedení předmětu díla, resp. jeho části, svolá zhotovitel přejímací řízení, kterým bude ukončeno akceptační řízení. V rámci přejímacího řízení budou předloženy všechny akceptační protokoly, přičemž žádný z nich nesmí obsahovat výsledek akceptace „Nesplněno“. Na přejímací řízení přizve zhotovitel objednatele, a to písemným oznámením.
- 4.10. Vlastnické právo k dílu přechází na objednatele okamžikem předání díla objednateli. Práva z poskytnuté licence objednatel nabývá okamžikem převzetí díla od zhotovitele.

#### **5. Cena a platební podmínky**

- 5.1. Cena díla vymezeného v čl. 2.1 je stanovena na základě nabídkové ceny zhotovitele, kalkulované v rámci veřejné zakázky a její podrobný rozpis tvoří přílohu č. 2 této smlouvy.
- 5.2. Cena díla činí částku ve výši 9 927 840 Kč bez DPH (slovy: devět milionů devět set dvacet sedm tisíc osm set čtyřicet korun českých). DPH ve výši 21 % činí 2 084 846,40 Kč slovy: dva miliony osmdesát čtyři tisíc osm set čtyřicet šest korun českých čtyřicet haléřů). Cena díla celkem včetně

DPH činí 12 012 686,40 Kč (slovy: dvanáct milionů dvanáct tisíc šest set osmdesát šest korun českých čtyřicet haléřů).

- 5.3. Takto ujednaná celková cena díla je cenou fixní, konečnou a závaznou za provedení díla. Rovněž jednotkové ceny uvedené v rozpisu, který tvoří přílohu číslo 2 této smlouvy, ze kterých se celková cena skládá, jsou cenami fixními, konečnými a závaznými.
- 5.4. Cena díla zahrnuje zejména dopravu, instalaci a implementaci a zprovoznění díla. Cena díla zahrnuje i náklady na správní poplatky, daně, cla, schvalovací řízení apod. (je-li relevantní), pojištění, přepravní náklady apod. Celková cena díla je stanovena dohodou smluvních stran a jako cena nejvýše přípustná.
- 5.5. Cenu díla je možné překročit pouze v souvislosti se změnou daňových předpisů upravujících výši DPH, přičemž v takovém případě bude ke kupní ceně připočteno DPH ve výši stanovené zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „zákon o dani z přidané hodnoty“).
- 5.6. Cena díla bude objednatelem uhrazena v korunách českých (CZK) na základě daňového dokladu (dále jen „faktura“) vystaveného zhotovitelem.
- 5.7. Přílohou faktury musí být kopie akceptačního protokolu souhrnného akceptačního řízení podepsaného osobami oprávněnými jednat za smluvní strany.
- 5.8. Faktura, musí obsahovat všechny náležitosti řádného daňového dokladu ve smyslu zákona o dani z přidané hodnoty. V případě, že faktura bude obsahovat věcné či formální nesprávnosti, popřípadě nebude obsahovat všechny zákonné náležitosti nebo přílohu dle předchozího odstavce, je objednatel oprávněn ji vrátit ve lhůtě splatnosti zpět zhotoviteli k doplnění či opravě, aniž se tak dostane do prodlení se splatností. Lhůta splatnosti počíná běžet ode dne vystavení náležitě doplněné či opravené faktury. Na faktuře bude uveden název a číslo projektu.
- 5.9. Fakturu, tak jak je výše uvedeno, je zhotovitel oprávněn vystavit až po řádném protokolárním převzetí kompletního díla objednatelem, tak jak jsou dohodnuty podmínky pro předání díla v článku 4 – Provedení a předání díla této smlouvy. Splátnost faktury se sjednává na 60 dnů ode dne vystavení faktury. Za den splnění povinnosti zaplatit cenu je považován den odepsání příslušné částky z účtu objednatele.
- 5.10. Objednatel neposkytuje zhotoviteli zálohy na cenu díla.
- 5.11. Smluvní strany se výslovně dohodly, že objednatel je oprávněn započíst své i nesplátné pohledávky vzniklé na základě této smlouvy proti pohledávce zhotovitele na zaplacení ceny díla rovněž bez ohledu na její splatnost.
- 5.12. Zhotovitel se zavazuje, že v případě nabytí statutu „nespolehlivý plátc“ ve smyslu zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, bude o této skutečnosti neprodleně objednatele informovat. Objednatel je poté oprávněn zaslat hodnotu plnění odpovídající dani z přidané hodnoty přímo na účet správce daně v režimu podle §109a zákona o dani z přidané hodnoty.

## **6. Práva a povinnosti stran**

- 6.1. Zhotovitel je povinen dodat objednateli úplné a funkční dílo dle této smlouvy, a pokud je součástí dodávky i zboží, bude se jednat o nové nepoužité zboží v dohodnutém množství, jakosti a provedení, které je zhotovitel povinen předložit v souladu se specifikací technických a uživatelských standardů a objednatelem písemně odsouhlasenou dokumentací.
- 6.2. Zhotovitel je povinen v souladu s podmínkami této smlouvy řádně a včas dodat objednateli dílo dle této smlouvy, a to včetně implementace, provedení potřebné montáže, instalace a zprovoznění na místě plnění, přičemž za řádné dodání díla se považuje jeho převzetí objednatelem, a to na základě potvrzení této skutečnosti v protokolu o předání a převzetí dodávky díla. Předávací protokol může

být podepsán nejdříve v okamžiku, kdy bude beze zbytku realizována dodávka díla zhotovitelem včetně dodání na místo určené objednatelem, instalace, implementace a zprovoznění díla.

- 6.3. Zhotovitel je povinen spolu s dílem dodat objednateli kompletní dokumentaci nezbytnou k užívání zboží, a to zejména záruční listy a návody a další dokumentaci požadovanou ve veřejné zakázce, přičemž je současně povinen provést proškolení obsluhy díla a potřebné revize.
- 6.4. Objednatel nabývá vlastnického práva k dílu dnem řádného předání a převzetí díla od zhotovitele na základě podpisu předávacího protokolu oběma smluvními stranami. Stejným okamžikem přechází na objednatele také odpovědnost za nebezpečí škody na zboží.
- 6.5. Zhotovitel je povinen neprodleně písemně vyrozumět objednatele o případném ohrožení doby plnění a o všech skutečnostech, které mohou řádné a včasné plnění předmětu této smlouvy znemožnit, a to nejpozději do 3 dnů ode dne, kdy se zhotovitel dozví o takové skutečnosti.
- 6.6. Zhotovitel není oprávněn postoupit jakákoliv práva anebo povinnosti vyplývající z této smlouvy na třetí osoby bez předchozího písemného souhlasu objednatele.
- 6.7. Smluvní strany sjednávají, že zhotovitel není oprávněn jakékoliv jeho pohledávky za objednatelem, které vzniknou na základě této smlouvy, započítat vůči pohledávkám objednatele za zhotovitelem jednostranným právním jednáním.
- 6.8. Zhotovitel odpovídá objednateli za škodu způsobenou porušením jakékoliv povinnosti podle této smlouvy nebo povinnosti stanovené obecně závazným platným právním předpisem.
- 6.9. Smluvní strany se dohodly a zhotovitel určil, že osobou oprávněnou k jednání za zhotovitele v technických věcech, které se týkají této smlouvy a její realizace, je/Jsou:
- Jméno a příjmení: Bc. Dagmar Krejzová  
e-mail: krejzova@stapro.cz  
tel.: +420 734 433 330
- 6.10. Smluvní strany se dohodly a objednatel určil, že osobou oprávněnou k jednání za objednatele v technických věcech, které se týkají této smlouvy a její realizace, je:
- Jméno a příjmení: Ing. Hana Vojtíšková  
e-mail: vojtiskova@nemkadan.cz  
tel.: +420 606 882 563
- 6.11. Veškerá korespondence, pokyny, oznámení, žádosti, záznamy a jiné dokumenty vzniklé na základě této smlouvy mezi smluvními stranami nebo v souvislosti s ní budou vyhotoveny v písemné formě v českém jazyce a doručují se buď osobně, doporučenou poštou, prostřednictvím datové schránky nebo v oprávněných případech e-mailem, na adresu sídla, ID datové schránky nebo e-mailové adresy kontaktních osob objednatele. Smluvní strany se v případě doručování zásilek formou doporučených dopisů dohodly tak, že zásilka je považována za doručenu 3. pracovní den bezprostředně následující po dni jejího odeslání prostřednictvím držitele poštovní licence na adresu příslušné smluvní strany dle záhlaví této smlouvy.
- 6.12. Zhotovitel je povinen ve lhůtě do 10 pracovních dnů ode dne nabytí účinnosti této smlouvy uzavřít pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti zhotovitele za škodu způsobenou zhotovitelem do výše limitu pojistného plnění v částce minimálně 10.000.000,- Kč z jedné pojistné události ročně. Zhotovitel se zavazuje na žádost objednatele bezodkladně, nejpozději však ve lhůtě do 5 pracovních dnů od doručení písemné výzvy objednatele, předložit objednateli pojistný certifikát prokazující existenci a účinnost této pojistné smlouvy. Zhotovitel se zavazuje, že pojistná smlouva dle věty první tohoto článku zůstane v účinnosti v tomto rozsahu po celou dobu trvání záruky. Za porušení povinnosti dle tohoto odstavce zaplatí zhotovitel objednateli smluvní pokutu ve výši 0,05 % z ceny díla bez DPH dle čl. IV. odst. 2) této smlouvy za každý, byť jen započatý den, v němž bude zhotovitel v prodlení. Zaplacením smluvní pokuty není dotčeno právo objednatele na uplatnění případného nároku na náhradu případně vzniklé škody.

- 6.13. Zhotovitel se zavazuje označovat veškeré vydané faktury názvem a číslem projektu uvedeným v Preambuli této smlouvy.
- 6.14. Zhotovitel je povinen minimálně do roku 2028 poskytovat požadované informace a dokumentaci související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.
- 6.15. Zhotovitel je povinen uchovávat veškerou dokumentaci související s realizací projektu včetně faktur minimálně do konce roku 2028. Pokud je v příslušných českých právních předpisech stanovena lhůta delší, musí ji zhotovitel použít.

#### **Součinnost**

- 6.16. Rozsah součinnosti bude specifikován a objednatelem odsouhlasen při zahájení realizace jako součást Dokumentace skutečného provedení (viz příloha č. 1 této smlouvy – Specifikace technického řešení).

#### **Realizační tým**

- 6.17. Zhotovitel se zavazuje předmět plnění smlouvy realizovat prostřednictvím projektového týmu, kterým prokázal kvalifikaci ve veřejné zakázce, na jejímž základě je uzavírána tato smlouva o dílo. Projektový tým zhotovitele je odpovědný za plnění této smlouvy o dílo.

### **7. Záruka za jakost**

- 7.1. Zhotovitel se zavazuje, že předaný předmět díla bude prostý vad a bude mít vlastnosti dle obecně závazných právních předpisů, této smlouvy a zadávací dokumentace veřejné zakázky uvedené v preambuli této smlouvy, dále bude mít vlastnosti první jakosti provedení a bude proveden v souladu s ověřenou technickou praxí.
- 7.2. Zhotovitel odpovídá za vady, které má předmět plnění v době jeho předání objednateli a za vady, které vzniknou nebo se objeví v průběhu záruční doby.
- 7.3. Zhotovitel poskytuje záruku na dílo specifikované v čl. 2.1 této smlouvy v souladu s Přílohou č. 1 – Specifikace technického řešení této smlouvy, a to v průběhu 24 měsíců na Software řešení a 36 měsíců na Hardware řešení od okamžiku protokolárního předání a převzetí díla objednatelem. Záruční doba začíná běžet ode dne převzetí díla objednatelem. Záruční doba se prodlužuje o dobu, po kterou mělo dílo vadu bránící jeho řádnému užívání objednatelem, nebo po kterou bylo plnění mimo provoz z důvodu vady, na kterou se vztahuje záruka.
- 7.4. Zhotovitelem bude objednateli poskytován bezplatný záruční servis na objednatelem reklamované vady předmětu díla vzniklé v době trvání záruční doby.
- 7.5. Objednatel je oprávněn reklamovat v záruční době vady předmětu díla u zhotovitele, a to písemnou formou. V reklamaci musí být popsána vada předmětu díla, určen nárok objednatele z vady předmětu díla, případně požadavek na způsob odstranění vad, a to včetně termínu pro odstranění vad zhotovitelem. Objednatel má právo volby způsobu odstranění důsledku vadného plnění. Za písemnou formu je považováno také nahlášení standardními prostředky technické podpory provozu, např. e-mailem nebo prostřednictvím aplikace HelpDesk. Aplikace HelpDesk je provozována v režimu 24/7.
- 7.6. Zhotovitel se zavazuje od okamžiku oznámení vady předmětu díla či jeho části zahájit odstraňování vady či jeho části v co nejkratší lhůtě, nejpozději do 3 dnů od uplatnění oprávněné reklamace objednatelem, a to i tehdy, neuznává-li zhotovitel odpovědnost za vady či příčiny, které ji vyvolaly, a vady odstranit v technicky co nejkratší lhůtě, a současně zahájit reklamační řízení v místě provádění předmětu díla. O reklamačním řízení budou objednatelem pořizovány písemné zápisy ve dvojnásobném vyhotovení, z nichž jeden stejnopis obdrží každá ze smluvních stran. Bude-li v reklamačním řízení vada uznána jako reklamační vada, bude odstranění vady předmětu díla či jeho části provedeno bezúplatně.

- 7.7. Objednatel má vůči zhotoviteli tato práva z odpovědnosti za vady:
- a) právo na bezplatné odstranění reklamovaných vad, a to bezprostředně po oznámení vady objednatelem, nejpozději ve lhůtě 30 dnů od oznámení vady objednatelem,
  - b) právo na poskytnutí přiměřené slevy z ceny odpovídající rozsahu reklamovaných vad či nedodělků,
  - c) právo na odstoupení od smlouvy, kdy vady či nedodělky jsou takového charakteru, že ztěžují či dokonce brání v užívání díla, nebo
  - d) právo na zaplacení nákladů na odstranění vad v případě, kdy si objednatel vadu či nedodělek odstraní sám nebo použije třetí osoby k jejich odstranění.
- 7.8. Zhotovitelem bude v souladu s Občanským zákoníkem poskytnuta záruka na příslušenství díla v podobě dodaného Hardware v délce trvání 24 měsíců. Záruka se nevztahuje na spotřební materiál tohoto příslušenství a komponenty tohoto příslušenství podléhající běžnému opotřebením.
- 7.9. Záruka se nevztahuje na vady prokazatelně způsobené neodbornou manipulací (nesprávnou obsluhou, nedodržením doporučených postupů nebo mechanickým poškozením) objednatelem.
- 7.10. Uplatněním nároků z odpovědnosti za vady není dotčeno právo na náhradu škody. Zhotovitel odpovídá objednateli za případnou škodu, která mu vznikne z titulu neodstranění vady díla zhotovitelem ve stanoveném termínu.
- 7.11. Záruka je poskytována v souladu s § 2113 a násl. Občanského zákoníku.

## **8. Licenční ujednání**

- 8.1. Zhotovitel v rámci plnění předmětu této smlouvy vytvoří dílo podléhající ochraně podle Autorského zákona, a Občanského zákoníku, a tak poskytuje objednateli licenci - tj. oprávnění k výkonu práva užívat jím vytvořené autorské dílo.
- 8.2. Zhotovitel poskytuje licenci jako:
- a) nevýhradní licenci k veškerým známým způsobům užití takového díla, zejména, nikoliv však výlučně k účelu, ke kterému bylo takové dílo zhotovitelem vytvořeno v souladu s touto smlouvou, a to v rozsahu minimálně nezbytném pro řádné užívání díla objednatelem,
  - b) licenci neomezenou územím výkonu působnosti objednatele,
  - c) licenci co do rozsahu oprávněného počtu uživatelů k užívání informačního systému a jeho jednotlivých oblastí neomezenou, nestanoví-li příloha č. 1 smlouvy – Specifikace technického řešení počty licencí pro jednotlivé moduly jinak;
  - d) neomezenou způsobem nebo rozsahem užití;
  - e) licenci udělenou na dobu neurčitou;
  - f) licenci, kterou není objednatel povinen využít.
- 8.3. Povinnost týkající se licence platí pro zhotovitele i v případě zhotovení části díla poddodavatelem.
- 8.4. Licence je poskytnutá v maximálním rozsahu povoleném platnými právními předpisy.
- 8.5. Zhotovitel je povinen zajistit, aby výsledkem jeho plnění nebo jakékoliv jeho části nebyla porušena práva třetích osob. Pro případ, že užíváním předmětu plnění nebo jeho dílčí části nebo prostou existencí předmětu plnění nebo jeho dílčí části budou v důsledku porušení povinností zhotovitele dotčena práva třetích osob, nese zhotovitel vedle odpovědnosti za takovéto vady plnění i odpovědnost za veškeré škody, které tím objednateli vzniknou.
- 8.6. Zhotovitel uděluje objednateli oprávnění dílo spojit s dílem jiným a s dílem dále pracovat za účelem jeho dalšího rozvoje a používání.

- 8.7. Objednatel a zhotovitel se výslovně dohodli, že odměna za veškerá licenční oprávnění poskytnutá objednateli je již zahrnuta v ceně za poskytnuté plnění dle této smlouvy, tj. cena za poskytnutí licence, včetně nákladů souvisejících s případnou aktualizací licence.
- 8.8. Licence k datům – veškerá data zpracovávaná nejen objednatelem v informačním systému jsou data objednatele a o nakládání s nimi rozhoduje výhradně objednatel.

## 9. Smluvní pokuty

- 9.1. V případě prodlení zhotovitele s řádným provedením a předáním díla v termínu dle této smlouvy postihuje objednatel zhotovitele smluvní pokutou ve výši 0,05 % z celkové ceny díla za každý i započatý den prodlení.
- 9.2. V případě prodlení zhotovitele se zahájením odstraňování řádně reklamované vady dle článku 7.6 této smlouvy postihuje objednatel zhotovitele smluvní pokutou ve výši 0,05 % z celkové ceny díla za každý den prodlení.
- 9.3. V případě prodlení objednatele s úhradou faktury je objednatel povinen uhradit zhotoviteli smluvní pokutu ve výši 0,05 % z dlužné částky za každý den prodlení.
- 9.4. V případě prodlení zhotovitele s doručením konečné faktury, postihuje objednatel zhotovitele smluvní pokutou ve výši 0,05 % z celkové ceny díla za každý den prodlení.
- 9.5. Smluvní pokuty výše uvedené jsou splatné do 10 dnů od doručení výzvy oprávněné strany k její úhradě.

## 10. Zvláštní ujednání

- 10.1. Smluvní strany berou na vědomí, že smlouva bude zveřejněna v registru smluv v souladu se zákonem č. 340/2015 Sb., o registru smluv, v platném znění. Zveřejnění provede odpovědný objednatel ve lhůtě 15 dnů ode dne podpisu smlouvy poslední smluvní stranou. Do 3 dnů pak protistranu informuje o splnění této povinnosti a o případných změnách a opravách provedených v registru smluv.
- 10.2. Odstoupit od smlouvy lze pouze z důvodů stanovených v této smlouvě nebo v Občanském zákoníku.
- 10.3. Od této smlouvy může smluvní strana dotčená porušením povinnosti jednostranně odstoupit pro podstatné porušení této smlouvy druhou smluvní stranou, přičemž za podstatné porušení této smlouvy se považuje:
- je-li objednatel v prodlení se zaplacením ceny díla podle této smlouvy po dobu delší než 30 dní po dni splatnosti příslušné faktury, ačkoliv byl na své prodlení písemně upozorněn a přes toto písemné upozornění objednatel nápravu neprovedl ve lhůtě do 10 dnů od doručení písemného upozornění;
  - jestliže zhotovitel dodá dílo, které nebude mít vlastnosti deklarované zhotovitelem v této smlouvě, resp. v nabídce zadávacího řízení, na jehož základě byla tato smlouva uzavřena;
  - jestliže zhotovitel dodá dílo, které je zatíženo právy třetích osob.
- 10.4. Objednatel je dále oprávněn od Smlouvy písemně odstoupit z důvodu jejího podstatného porušení, přičemž za podstatné porušení Smlouvy se bude považovat opakované (alespoň 3 x za příslušné kalendářní pololetí) prodlení poskytovatele s dodržením požadované maximální doby zahájení řešení či maximální doby odstranění záruční vady kategorie A či s dodržením požadované maximální doby odezvy či maximální doby odstranění incidentu kategorie A, tj. poskytovatel nedodrží lhůty tam uvedené pro tuto kategorii vad/incidentů oproti lhůtám tam stanoveným o více než 24 hodin.
- 10.5. Objednatel je rovněž oprávněn odstoupit od Smlouvy v případě, že:
- v insolvenčním řízení bude zjištěn úpadek poskytovatele nebo insolvenční návrh bude zamítnut pro nedostatek majetku poskytovatele v souladu se zněním zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů.



Objednatel je rovněž oprávněn odstoupit od Smlouvy v případě, že poskytovatel vstoupí do likvidace; nebo

- b) proti poskytovateli je zahájeno trestní stíhání pro trestný čin podle zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob, ve znění pozdějších předpisů.

- 10.6. Odstoupením od této smlouvy zanikají všechny závazky smluvních stran z této smlouvy. V případě odstoupení od této smlouvy nezanikají nároky smluvních stran na náhradu škody a zaplacení smluvních pokut sjednaných pro případ porušení smluvních povinností vzniklé před skončením účinnosti této smlouvy, a ty závazky smluvních stran, které podle smlouvy nebo vzhledem ke své povaze mají trvat i nadále, nebo u kterých tak stanoví občanský zákoník.
- 10.7. Odstoupení od smlouvy musí být učiněno v písemné formě a nabývá účinnosti dnem jeho doručení druhé smluvní straně.

## **11. Ochrana informací**

- 11.1. Zhotovitel se zavazuje, že zachová jako citlivé informace a zprávy týkající se vnitřních záležitostí smluvních stran a předmětu plnění smlouvy, pokud by jejich zveřejnění mohlo poškodit druhou stranu. Povinnost poskytovat informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, není tímto ustanovením dotčena.
- 11.2. Smluvní strany budou považovat za citlivé informace a) jako citlivé označené, b) informace, u kterých se z povahy věci dá předpokládat, že se jedná o informace podléhající závazku mlčenlivosti nebo informace o objednateli, které by mohly z povahy věci být považovány za citlivé a které se dozvědí v souvislosti s plněním této smlouvy.
- 11.3. Smluvní strany se zavazují, že neuvolní třetí osobě informace druhé strany bez jejího souhlasu, a to v jakékoliv formě, a že podniknou všechny nezbytné kroky k zabezpečení těchto informací. Závazek mlčenlivosti a ochrany citlivých informací zůstává v platnosti po dobu 5 let po ukončení platnosti smlouvy.
- 11.4. Zhotovitel je povinen zabezpečit veškeré podklady, mající charakter citlivé informace poskytnuté mu objednatel, proti odcizení nebo jinému zneužití.
- 11.5. Zhotovitel je povinen svého případného poddodavatele zavázat povinností mlčenlivosti a respektováním práv objednatele nejméně ve stejném rozsahu, v jakém je v závazkovém vztahu zavázán sám.
- 11.6. V souvislosti s důvěrností informací bere zhotovitel na vědomí, že je zákonnou povinností objednatele uveřejnit celé znění této smlouvy včetně všech jejích případných dodatků a seznamu subdodavatelů v souladu se zákonem. Splnění této, jakož i dalších zákonných povinností objednatele, není porušením důvěrnosti informací.
- 11.7. Povinnost zachovávat mlčenlivost se nevztahuje na informace:
- a) které jsou nebo se stanou všeobecně a veřejně přístupnými jinak, než porušením ustanovení tohoto odst. ze strany zhotovitele,
  - b) které jsou zhotoviteli známy a byly mu volně k dispozici ještě před přijetím těchto informací od objednatele,
  - c) které budou následně zhotoviteli sděleny bez závazku mlčenlivosti třetí stranou, jež rovněž není ve vztahu k nim nijak vázána,
  - d) jejichž sdělení se vyžaduje ze zákona.
- 11.8. Za prokázané porušení ustanovení v tomto čl. má druhá smluvní strana právo požadovat náhradu takto vzniklé škody ve výši 100.000,- Kč za každé porušení povinností.

## **12. Závěrečná ustanovení**

- 12.1. Uhrazením smluvní pokuty není dotčeno právo objednatele na náhradu škody, kterou zhotovitel způsobil objednateli nesplněním svých povinností, ke kterým se zhotovitel zavázal v této smlouvě.

Smluvní strany tímto, po vzájemné dohodě, vylučují použití § 2050 Občanského zákoníku. Smluvní pokuty dle této smlouvy jsou splatné do 10 dnů od doručení výzvy oprávněné strany k její úhradě.

Pro případ, že by byla smluvní pokuta soudem snížena, dohodly se zároveň smluvní strany, že zůstává zachováno právo na náhradu škody ve výši, v jaké škoda převyšuje částku určenou soudem jako přiměřenou. Smluvní pokuty dle této smlouvy lze požadovat kumulativně, a to bez omezení. Úhradou smluvní pokuty zhotovitelem není dotčena další existence povinnosti smluvní pokutou zajištěné. Smluvní pokuta dle této smlouvy je splatná do 15 kalendářních dnů ode dne doručení písemného uplatnění práva na smluvní pokutu, a to na účet písemně určený objednatelem. Smluvní pokutu je objednatel oprávněn započíst oproti splatným pohledávkám zhotovitele.

- 11.2. Smluvní strany se dohodly, že nejsou oprávněny převést práva a povinnosti z této smlouvy na třetí osobu bez předchozího písemného souhlasu druhé smluvní strany.
- 11.3. Součástí povinností zhotovitele je i závazek k uzavření budoucí Smlouvy o zpracování osobních údajů nebo jiné smlouvy dle požadavku objednatele, kterou zhotovitel uzavře s objednatelem v případě, že k tomu bude objednatelem vyzván, jako závazku z plnění souvisejících se zpracováním osobních údajů vč. citlivých podle 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) – dále také „Nařízení GDPR“.
- 11.4. Tato smlouva nabývá platnosti dnem podpisu poslední ze smluvních stran a účinnosti okamžikem jejího uveřejnění v registru smluv. Smluvní strany berou na vědomí, že tato smlouva vyžaduje uveřejnění v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a registru smluv, ve znění pozdějších předpisů a s tímto uveřejněním souhlasí. Zaslání smlouvy do registru smluv se objednatel zavazuje zajistit neprodleně po podpisu smlouvy.
- 11.5. Vztahy mezi smluvními stranami se řídí českým právním řádem. Ve věcech smlouvou výslovně neupravených se právní vztahy z ní vznikající a vyplývající řídí příslušnými ustanoveními Občanského zákoníku a ostatními obecně závaznými právními předpisy. Rozhodčí řízení je vyloučeno.
- 11.6. Nastanou-li u některé ze smluvních stran skutečnosti bránící řádnému plnění této smlouvy, je povinna to ihned bez zbytečného odkladu písemně oznámit druhé smluvní straně a vyvolat jednání objednatele a zhotovitele.
- 11.7. Vztahuje-li se důvod neplatnosti jen na některé ustanovení smlouvy, je neplatným pouze toto ustanovení, pokud z jeho povahy, obsahu anebo z okolností, za nichž bylo sjednáno, nevyplývá, že jej nelze oddělit od ostatního obsahu smlouvy. Smluvní strany se zavazují, že bezodkladně nahradí neplatné ustanovení této smlouvy jiným platným ustanovením svým obsahem podobným neplatnému ustanovení.
- 11.8. Smlouva se vyhotovuje ve 3 stejnopisech, z nichž každý má platnost originálu, přičemž Objednateli přináležejí dva stejnopisy a Zhotoviteli 1 stejnopis.
- 11.9. Nedílnou součástí této smlouvy jsou následující přílohy:
  - a) Příloha č. 1 – Specifikace technického řešení
  - b) Příloha č. 2 – Položkový rozpočet
  - c) Příloha č. 3 – Závazný harmonogram plnění
  - d) Příloha č. 4 – Zadávací dokumentace [*příloha pevně nesvázaná, připojená na datovém nosiči*]

V Kadani dne \_\_\_\_\_

V Pardubicích dne .....

Za Objednatele:

Nemocnice Kadaň s.r.o.

.....

MUDr. Bc. Petr Hossner, MBA

jednatel

Za Zhotovitele:

.....

Ing. Leoš Raibr

jednatel společnosti STAPRO s. r. o.

## **PŘÍLOHA Č. 1 SMLOUVY O DÍLO - Specifikace technického řešení** (dále jen „příloha“)

uzavřená ve smyslu ust. § 2586 a násl. a ust. § 1746 zákona č. 89/2012 Sb., občanského zákoníku (dále jen „Občanský zákoník“), ve znění pozdějších předpisů a podle zákona č. 121/2000 Sb. (dále jen „autorský zákon“), ve znění pozdějších předpisů

### **Objednatel:**

Nemocnice Kadaň s.r.o.

se sídlem: Golovinova 1559, 432 01 Kadaň  
IČ: 25479300  
ID datové schránky: z28pu9r  
jednající: MUDr. Bc. Petr Hossner, MBA, jednatel  
bankovní spojení: UniCredit Bank Czech Republic and Slovakia, a.s.  
číslo účtu: 155977/2700

### **Zhotovitel nebo Účastník:**

STAPRO s. r. o.

se sídlem: Pernštýnské náměstí 51, 530 02 Pardubice  
IČ: 13583531  
DIČ: CZ699004728  
za níž jedná: Ing. Leoš Raibr, jednatel společnosti STAPRO s. r. o.  
zapsaná v Obchodním rejstříku vedeném Krajským soudem v Hradci Králové spisová značka C 148  
tel.: +420 467 003 111 fax.: +420 467 003 119, e-mail: obchod@stapro.cz  
bankovní spojení: ČSOB a.s. / Oberbank AG  
číslo účtu: 271810793/0300 / 2171133923/8040  
dále společně jako „smluvní strany“

## **Podrobný popis projektu**

### **1. Podrobný popis výchozího stavu**

Objednatel v tuto chvíli nedisponuje žádným portálovým řešením, které by umožňovalo elektronickou výměnu dat s pacientem či zaměstnancem Objednatele.

Vzhledem k požadavkům klientů objednatele a také nárůstu počtu pacientů se ve stále větší míře vyskytuje potřeba jednat s pacienty/zaměstnanci elektronicky bez nutnosti fyzické návštěvy či telefonického hovoru. Tato potřeba je dále umocněna vzrůstající cenou práce, která zvyšuje cenu individuálně poskytovaných administrativních služeb. Cílem organizace je tedy zvýšit efektivitu poskytovaných služeb.

Smyslem projektu je vybudování nového portálového řešení, které bude napojené na interní provozní systémy (NIS, LIS, PACS, DocReg) a dohledové systémy (LOG management...).

Umožnit pacientům a zaměstnancům činit digitální úkony bez nutnosti fyzické návštěvy Nemocnice Kadaň s.r.o. (získání zdravotnické dokumentace, zpráv). Jde tedy o zvýšení efektivitu a dostupnosti částí poskytovaných služeb.

V současné době je situace taková, že se pacient objednává k převzetí své zdravotnické dokumentace, která může být nedigitalizovaná, tudíž nepředatelná portálovým systémem. Zaměstnanci nemocnice musí tuto dokumentaci předem fyzicky shromáždit, nakopírovat, připravit atd., což je samozřejmě časově i

finančně náročné, zvyšuje to riziko chyb a také neumožňuje to personálu nemocnice provádět další nezbytné činnosti.

### 1.1 Výčet IS, KS a ICT vybavení OBJEDNATELE

Objednatel spravuje následující informační systémy:

- Nemocniční informační systém STAPRO FONS Akord
- Laboratorní informační systém STAPRO OpenLIMS
- Mzdový a personální systém Vema – Solitea
- Stravovací provoz – objednávání a výdej stravy – STAPRO FONS Akord
- Ekonomický systém Helios ECODATE
- Manažerský informační systém – STAPRO MIS
- Správa, ukládání (archivace) a zobrazení obrazové dokumentace – MARIE PACS

Výše uvedené informační systémy jsou v současné době do značné míry izolované a velmi často dochází k duplicitám a neefektivitám, kdy je nutné např. dokumentaci pacienta fyzicky předávat, což s sebou samozřejmě nese rizika ztrát, chybovosti apod. Celkově je míra elektronizace, automatizace, centralizace a standardizace na velmi nízké úrovni, což má vliv jak na interní chod nemocnice, tak i směrem „ven“ při kontaktu s klienty (pacienty), vykazování pro zakladatele, napojení na eHealth KÚ Ústeckého kraje, pojišťovny, Český statistický úřad, či jiná zdravotnická zařízení a úřady. Tento obecně popsáný nepříznivý stav je dále rozepsán dle jednotlivých (požadovaných) nového IS – a to ve formě uvedení požadovaných parametrů a funkcionalit, kterými stávající IS nedisponují.

### 1.2 Popis jednotlivých částí PORTÁLU

<b>Název pořizovaného IS</b>	<b>Transakční portál pro sdílení a výměnu dat vč. napojení na eHealth systém kraje a auditních služeb</b>
<b>ID IS</b>	IS 1
<b>Aktivita dle kapitoly 2.3 specifických pravidel výzvy</b>	<p>Realizace projektu naplňuje tyto aktivity dle kapitoly 2.3 Specifických pravidel:</p> <ol style="list-style-type: none"> <li>1. Opatření vedoucí k intenzivnímu využívání existujících bezpečných systémů elektronické identifikace</li> <li>2. Transakční portálová řešení s využitím zaručené elektronické identity</li> <li>3. Automatizace zpracování digitálních dat (robotizace)</li> </ol> <p>Ad 1: Nově navržený portál bude zpracovávat transakční údaje z příslušných agendových informačních systémů. K přenosu dat mezi portálem a agendovými informačními systémy je použito šifrování. Bude taktéž využita autentizace uživatelů prostřednictvím služeb NIA. V systému vystupují všechny subjekty v roli uživatel autentizovaný. Neautentizovaný uživatel bude moci využívat portál pouze k nalezení informací např. na úřední desce apod.</p> <p>Ad 2:</p>

	<p>Hlavní aktivita projektu – smyslem projektu, který vede k naplňování dané aktivity, je poskytnout klientům a pracovníkům Objednatele možnost činit digitální úkony a snížit administrativní náročnost poskytovaných služeb a zároveň zvýšit jejich efektivitu a dostupnost. Jak bylo uvedeno výše, bude využito zaručené elektronické identity.</p> <p>Ad 3:</p> <p>Část operací, které bude portál zajišťovat, bude probíhat automaticky a nebude potřeba je vkládat do systému(ů) a ověřovat jejich správnost.</p> <p>V rámci projektu půjde dále o napojení na eHealth systém Ústeckého kraje a dále také o:</p> <ul style="list-style-type: none"> <li>- publikování osobních, demografických a dalších údajů pacienta (např. evidované kontakty apod.) z databáze NIS a dalších systémů prostřednictvím konsolidovaného kmene pacientů (MPI) na základě el. identity uživatele,</li> <li>- publikování údajů patientského souhrnu, tj. soubor údajů ze zdravotnické dokumentace stanovených platnou vyhláškou o zdravotnické dokumentaci,</li> <li>- publikování vybraných částí zdravotnické dokumentace vyhledané z NIS a DocReg, online objednání předání zdravotnické dokumentace</li> </ul> <p>Portál umožní předávání dat ve standardizované formě, která umožní další snadné zpracování (porovnatelnost, vytěžování...) ze strany centrálních orgánů (Ústecký kraj, ČSÚ apod.).</p> <p>Bude se jednat o nový IS, který dosud není v nemocnici využíván.</p> <p>HW a SW požadavky na systém nebudou vybočovat ze standardních požadavků na kancelářské vybavení, aby tak bylo umožněno jeho využívání na stávajícím vybavení v rámci Nemocnice Kadaň, s.r.o. (které je do značné míry různorodé kvality, stáří apod.).</p>
--	--

Níže jsou uvedeny požadavky na základní funkcionality tohoto systému:

### Transakční portál pro sdílení a výměnu dat

Požadavky na tuto část projektu jsou následující:

#	Požadavek
P.1	Součástí řešení bude vybudování otevřeného prostředí transakčního webového portálu využívajícího metod elektronické identifikace a autentizace občana garantovaných státem prostřednictvím služeb NIA.
P.2	Jsou požadovány tyto digitální služby integrované do uživatelského prostředí portálu <ol style="list-style-type: none"> <li>1. publikování osobních, demografických a dalších údajů pacienta (např. evidované kontakty apod.) z databáze NIS a dalších systémů prostřednictvím konsolidovaného kmene pacientů (MPI) na základě el. identity uživatele,</li> <li>2. publikování údajů patientského souhrnu, tj. soubor údajů ze zdravotnické dokumentace stanovených platnou vyhláškou o zdravotnické dokumentaci,</li> <li>3. publikování vybraných částí zdravotnické dokumentace vyhledané z NIS a DocReg,</li> </ol>

#	Požadavek
P.3	Portál bude webová aplikace, která bude dostupná pacientům a zdravotníkům prostřednictvím standardních webových prohlížečů, a která umožní snadný přístup ověřeného identifikovaného pacienta k dalším službám portálu.
P.4	Vytvoření komunikačních rozhraní a jejich integrace do NIS. LIS a PACS pro zprostředkování dat a služeb IS zadavatele do webového uživatelského prostředí portálu.
P.5	Řešení musí umožnit pacientům a praktickým lékařům zabezpečený vzdálený autorizovaný přístup k vybraným informacím ze zdravotnické dokumentace o jim poskytnutých zdravotních službách a jejich výsledcích formou náhledu na data z KIS.
P.6	Řešení musí zahrnovat jednoduché a dynamické uživatelské rozhraní, které nevyžaduje žádné proškolení uživatelů a je dostupné zabezpečeným způsobem přes internet prostřednictvím běžných webových prohlížečů (Firefox, Internet Explorer, Google Chrome, Safari) ve verzi dostupné v době implementace. Design uživatelského rozhraní bude navržen tak, aby v případě použití dotykového zařízení a prohlížeče podporujícího ovládání pomocí dotykového zařízení bylo ovládání ergonomické (usnadňovalo ovládání dotykem). Uživatelské rozhraní bude umožňovat rozpoznání velikosti obrazovky a přizpůsobí zobrazení velikosti této obrazovky, aby bylo použitelné i pro menší rozlišení.
P.7	Domovská stránka musí po přihlášení uživatele (pacienta) zobrazovat relevantní údaje o pacientovi, jako např. jeho demografické údaje a odkazy na další sekce s aktuálními informacemi z poskytnutých zdravotních služeb.
P.8	<p>Přihlášení k účtu uživatele (uživatelskému profilu), tzn. proces identifikace a autentizace uživatele, bude podporovat i alternativní metody přihlášení, konkrétně využití služeb NIA, pokud to v době realizace dodávky bude legislativně a technicky možné.</p> <p>Pro zvýšení bezpečnosti přístupu k údajům ze zdravotnické dokumentace je požadována</p> <ol style="list-style-type: none"> <li>1. více faktorová autentizace (např. zadáním kódu doručeného v SMS),</li> <li>2. fyzické ověření elektronické identity uživatele pověřeným pracovníkem nemocnice před aktivací oprávněnosti přístupu (jako náhrada dosud neexistující infrastruktury důvěryhodné externí identity).</li> </ol> <p>Více faktorová autentizace a ověření identity nejsou vyžadovány, pokud uživatel bude využívat pouze službu online, která navíc může být dostupná i pro neregistrované a nepřihlášené uživatele – v tomto případě s omezením jen na funkci odeslání objednávky s rezervací termínu a času.</p> <p>Naopak přístup ke zdravotnické dokumentaci a ostatním službám musí být umožněny pouze uživatelům s ověřenou identitou.</p> <p>Veškeré přístupy, zejména ke zdravotnickým informacím, musí být logovány a zaznamenány do auditního logu.</p>
P.9	Komunikace s NIS musí probíhat online.
P.10	<p>Webové uživatelské prostředí musí obsahovat hlavní navigační menu, které poskytne rychlý přístup do hlavních oblastí, jako např.:</p> <ol style="list-style-type: none"> <li>1. přehled poskytnutých zdravotních služeb,</li> <li>2. osobní data a nastavení,</li> <li>3. souhrnný elektronický zdravotní záznam pacienta vybraných údajů ze zdravotnické dokumentace,</li> </ol>

#	Požadavek
P.11	<p>Řešení musí zobrazit souhrnnou kartu, na které bude uveden přehled zdravotních údajů o pacientovi. Souhrnný elektronický zdravotní záznam pacienta musí obsahovat údaje vedené o pacientovi v rozsahu:</p> <ol style="list-style-type: none"> <li>1. osobní, demografické a kontaktní údaje,</li> <li>2. emergentní údaje (anamnézy, alergie, rizikové faktory, akutní diagnózy, akutní medikace),</li> <li>3. přehled ambulantních a hospitalizačních případů s možností zobrazení výstupních lékařských zpráv z poskytnutých zdravotních služeb (v případě existence dokumentu ve formě EZD také přístup k této formě dokumentu),</li> <li>4. patientský souhrn v souladu s metodikami vedení tzv. „elektronického patientského souhrnu“.</li> <li>5. Další standardizované dokumenty dle MZČR (Propouštěcí zpráva, Zpráva z obrazového vyšetření, Laboratorní zpráva) viz <a href="https://ncez.mzcr.cz/cs/standardy-elektronickeho-zdravotnictvi">https://ncez.mzcr.cz/cs/standardy-elektronickeho-zdravotnictvi</a></li> </ol> <p>Zobrazovány budou jen a pouze zprávy a dokumentace, které jsou finální, ověřené a potvrzené oprávněnou osobou v NIS, případně elektronicky podepsané a archivované.</p>
P.12	<p>Řešení musí nabízet funkci automatického zasílání upozornění pacientům formou emailových zpráv anebo SMS zpráv. Seznam všech archivovaných upozornění a varování musí být také součástí řešení. Vlastní doručování e-mailových zpráv a SMS zpráv není předmětem plnění a bude zajištěno zadavatelem separátně. Předmětem plnění je jen integrace na poskytnutá rozhraní systémů nebo služeb pro distribuci.</p>
P.13	<p>Řešení musí umožnit uživateli zaznamenat a měnit osobní údaje.</p>
P.14	<p>Otevřené prostředí portálu musí umožňovat rozšiřování o nové digitální služby pro pacienty.</p>

#### Výměna obrazové (PACS) dokumentace

#	Požadavek
P.15	<p>Řešení zajistí výměnu obrazové dokumentace mezi jinými ZZ resp. sítěmi pro výměnu dat pomocí HL7 protokolu (služba DocReg) a systémy nemocnice (PACS, NIS, Portál).</p>
P.16	<p>Řešení umožní přenést snímek do NIS a transakčního portálu. Z NIS i z portálu bude možné vyvolat webový prohlížeč snímků (prostřednictvím Accession number) a umožnit náhled v tomto prohlížeči.</p>
P.17	<p>Náhled bude umožněn lékaři v rámci NIS, ověřenému pacientovi v rámci portálu a pověřenému praktickému lékaři.</p>
P.18	<p>Snímek bude možné pomocí portálu předat ověřenému praktickému lékaři nebo specialistovi.</p>



## Napojení na eHealth systém kraje

Součástí projektu je napojení na eHealth systém Ústeckého kraje (dále ÚSK) v následujícím rozsahu funkcionalit:

#	Požadavek
P.19	Napojení na eHealth systém Ústeckého kraje
P.20	Vyhledání a poskytnutí patientského souhrnu pro eH NCP (demografické údaje, trvalé diagnózy, alergie, rizikové faktory, trvalé medikace, přehled ambulantních a hospitalizačních případů).
P.21	Vyhledání a poskytnutí vyžádané ambulantní a propouštěcí zprávy (online) -s příslušným stupněm ověření uživatele.
P.22	Příjem a import výjezdové zprávy ZZS do nemocnice.
P.23	Export a předání ambulantní a propouštěcí zprávy do eHealth (pro náhled na propouštěcí a ambulantní zprávy při výjezdu ZZS a pro předání do jiného ZZ).
P.24	Výměna dat mezi zdravotnickými zařízeními včetně dokumentů zdravotnické dokumentace vedené v elektronické formě.
P.25	Sdílení dat o zdravotní péči mezi zdravotnickými zařízeními (import / export ambulantních a propouštěcích zpráv).
P.26	Příjem a import výsledků z vyšetření ambulantního typu.
P.27	<p>V rámci integrace na eHealth ÚSK musí být splněny následující požadavky napojení vyžadované ze strany eHealth ÚSK pro napojení na NCP eH a NIX ZD:</p> <ol style="list-style-type: none"><li>1. Poskytování dat do eHealth ÚSK v rozsahu vyžadovaném ze strany NCP eH dle popisu implementace API národního konektoru NCPeH v příloze č. 4 na následující adrese: <a href="https://www.nixzd.cz/standard">https://www.nixzd.cz/standard</a>.</li><li>2. Poskytování dat do eHealth ÚSK v souladu s požadavky na vytvoření a ověření vzorového souboru patientského souhrnu (PS) ve formátu HL7 (CDA L3, ev. CDA L1) – vzory viz <a href="https://www.nixzd.cz/pacientsky_souhrn">https://www.nixzd.cz/pacientsky_souhrn</a>.</li><li>3. Poskytování dat do eHealth ÚSK v souladu s požadavky na PS CDA L1 a L3.</li></ol> <p>Po splnění uvedených požadavků bude Objednatelem od provozovatele NCP eH vyžádán protokol ověřující správnou realizaci uvedených požadavků a prokazující naplnění funkcionality interoperability dodávaného systému.</p>
P.28	<p>Výměna elektronické zdravotnické dokumentace prostřednictvím eHealth ústeckého kraje (dále ÚSK) s dalšími subjekty a systémy (ZZ, NIX ZD a eH NCP).</p> <ol style="list-style-type: none"><li>a. Předmětem dodávky je Integrace (připojení) NIS zdravotnického zařízení na Komunikační centrum Ústeckého kraje (dále KC ÚSK) a bude realizována v plné šíři, tj. komunikace se ZZS ÚSK, komunikace s ostatními ZZ ÚSK (případně jinými ZZ, pokud to KC ÚSK umožní), komunikace s pacienty v rozsahu předání zprávy a možnosti přenesení potřebných dat pro Patient Summary. Datové rozhraní pro předávání dat mezi NIS a KC bude v datovém standardu DASTA (verze 4). Výměna dat bude probíhat online nebo asynchronně podle služeb KC. Podporované musí být následující případy užití:</li></ol>

#	Požadavek
	<ul style="list-style-type: none"> <li>a. Vyhledání a poskytnutí životních údajů pacienta pro eH NCP (demografické údaje, trvalé diagnózy, alergie, rizikové faktory, trvalé medikace, přehled ambulantních a hospitalizačních případů) (online)</li> <li>b. Vyhledání a poskytnutí patientského souhrnu pro eH NCP (demografické údaje, trvalé diagnózy, alergie, rizikové faktory, trvalé medikace, přehled ambulantních a hospitalizačních případů) (online)</li> <li>c. Vyhledání a poskytnutí vyžádané ambulantní a propouštěcí zprávy (online)</li> <li>d. Příjem a import výjezdové zprávy ZZS (asynchronně)</li> <li>e. Příjem a import ambulantní a propouštěcí zprávy (asynchronně)</li> <li>f. Příjem a import výsledků z vyšetření ambulantního typu (asynchronně)</li> <li>g. Export a předání ambulantní a propouštěcí zprávy (asynchronně)</li> </ul> <p>Součástí integrace s KC bude také integrace (provolání) webového prohlížeče, který je součástí KC ÚSK, umožňujícího náhled na životní údaje pacienta u jiných poskytovatelů. V rámci NIS musí být zajištěna oprávněnost pro vyvolání této funkce na základě splnění podmínek vycházejících z legislativy o přístupu k informacím ze zdravotnické dokumentace jiného poskytovatele zdravotních služeb (uživatel poskytuje pacientovi lékařskou službu a je oprávněn k nahlížení z důvodu kontinuity lékařské péče).</p>
<b>P.29</b>	<p>Schopnost předávat výsledky vyšetření a zprávy praktickým lékařům a ambulantním specialistům dalšími způsoby – MISE/TransMISE, MedicalNet, atp. Tam kde je to možné, kontrola úplnosti údajů dle požadavků pracoviště či legislativy (především u RTG vyšetření):</p> <p>Export výsledků vyšetření a lékařských zpráv ve formátu DASTA ve verzi podporované příjemcem (předpokládá se maximálně verze 3 a 4) do definovaných adresářů s možností určování adresáře dle příjemce</p>
<b>P.30</b>	<p>Provázanost služby B2B kapitace na identifikační údaje (příjmení, jméno, IČP, adresa, aj.) praktického lékaře/specialisty v NIS a možnosti odesílat zprávy a výsledky.</p>

#### Auditní služby

Požadavky na tuto část NIS jsou následující:

#	Požadavek
<b>P.31</b>	<p>Navržená softwarová aplikace umožní provádět audity užití na základě interních logů aplikace, které zaznamenávají a ukládají údaje o změnách či nahlížení do patientské dokumentace podle identity uživatelů.</p>
<b>P.32</b>	<p>Řešení umožní poskytovat auditní reporty o přístupech uživatelů (kdo, kdy, období, kam) na základě parametrizace prováděné pověřeným auditorem.</p>
<b>P.33</b>	<p>Auditní (logovací) aparát je nezávislý a dostupný pouze určené roli (auditor). Není dostupný a manipulovatelný uživateli.</p>
<b>P.34</b>	<p>Systém musí umožnit automatizované i manuální vystoupení logových záznamů do integrační sběrnice (ESB), externích systémů pro správu logů (log management, SIEM) a do tabulek MS Excel (.csv, .xlsx).</p>

#	Požadavek
P.35	Auditní systém musí být v souladu s nařízením EU o ochraně osobních dat (GDPR).

**Tento IS bude zajišťovat níže uvedených 5 funkcionalit (uvedeno vč. stručného zdůvodnění způsobu tohoto zajištění):**

1. zvýšená spolehlivost, bezpečnost a průchodnost provozních informačních systémů, spravovaných jednotlivými OVM s využitím sdílení ICT platformem;

*Nový portál bude zabezpečen na vysoké úrovni, bude využívat více faktorovou autentizaci, fyzické ověření elektronické identity, šifrování apod.*

2. lepší dostupnost služeb veřejné správy nebo interoperabilita na území státu s přesahem v rámci EU;

*Nově budou služby portálu pro klienty dostupnější bez nutnosti fyzické přítomnosti v nemocnici, bude zajištěna interoperabilita a výměna dat pro účely dalších zapojených subjektů.*

3. využívání služeb národního bodu pro identifikaci a autentizaci;

*Viz výše – tento způsob identifikace a autentizace bude součástí vlastností nového portálu.*

4. zavedení metod automatizace a robotizace ve veřejné správě;

*Část operací a komunikace se stávajícími IS v rámci nemocnice bude zcela automatizovaná a bude tak zajištěna jejich bezproblémová funkčnost.*

5. budování informačního systému veřejné správy s podporou samostatných a oddělených modulů (kontejnerů) komunikujících pomocí mikroslužeb se zabráněním vendor lock-in.

*Nový IS bude využívat stávající data agendových IS v nemocnici a bude je agregovat a dále zpracovávat. Tyto funkce budou samostatnou součástí portálu a budou se stávajícími IS komunikovat pomocí integračních nástrojů*

Konečným stavem po realizaci projektu je implementace portálového řešení, dostupného pro pacienty/zaměstnance případně další oprávněné osoby Objednatele se zabezpečeným přístupem, jasnou identifikací identity uživatele poskytující následující služby:

1. publikování osobních, demografických a dalších údajů pacienta (např. evidované kontakty apod.) z databáze NIS a dalších systémů prostřednictvím konsolidovaného kmene pacientů (MPI) na základě elektronické identity uživatele,
2. publikování údajů patientského souhrnu, tj. soubor údajů ze zdravotnické dokumentace stanovených platnou vyhláškou o zdravotnické dokumentaci,
3. publikování vybraných částí zdravotnické dokumentace vyhledané z NIS a DocReg.

Portálové řešení bude integrováno s eHealth systémem Ústeckého kraje (poskytnutí patientského souhrnu, vyhledání vyžádané ambulantní/propouštěcí zprávy, výjezdové zprávy ZZS, výměna zdravotnické dokumentace).

V rámci integrace na eHealth ÚSK budou dodrženy požadavky vyžadované ze strany eHealth ÚSK pro napojení na NCP eH a NIX ZD:

4. Poskytování dat do eHealth ÚSK v rozsahu vyžadovaném ze strany NCP eH dle popisu implementace API národního konektoru NCPeH v příloze č. 4 na následující adrese: <https://www.nixzd.cz/standard>.

5. Poskytování dat do eHealth ÚSK v souladu s požadavky na vytvoření a ověření vzorového souboru patientského souhrnu (PS) ve formátu HL7 (CDA L3, ev. CDA L1) – vzory viz [https://www.nixzd.cz/pacientsky\\_souhrn](https://www.nixzd.cz/pacientsky_souhrn).
6. Poskytování dat do eHealth ÚSK v souladu s požadavky na PS CDA L1 a L

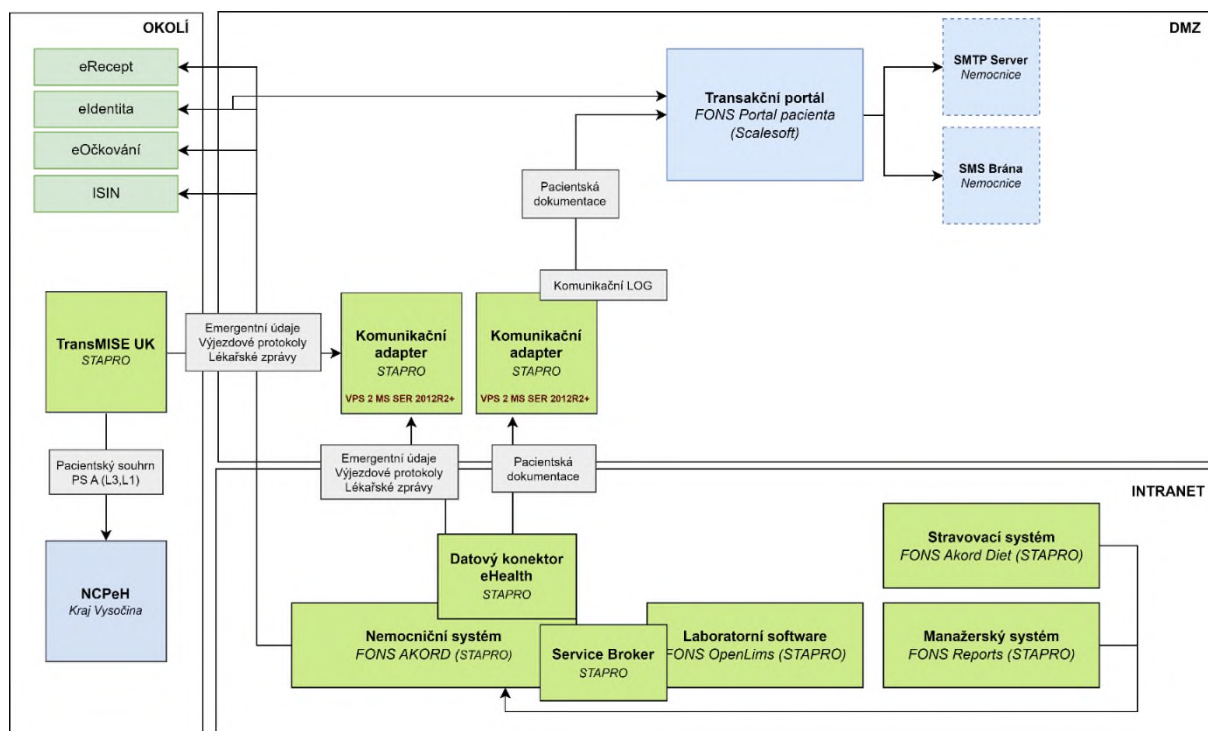
### 1.3 Firewall

Objednatel je nucen pro provoz transakčního portálu zajistit zvýšení funkcionality stávajícího řešení firewallu. Firewall je s ohledem na předmět projektu hlavní a klíčový prvek, zajišťující bezpečnost provozu sítě a prostředí, na kterém bude transakční portál provozován. Bez tohoto software není technicky možné zajistit bezpečný a spolehlivý provoz portálu.

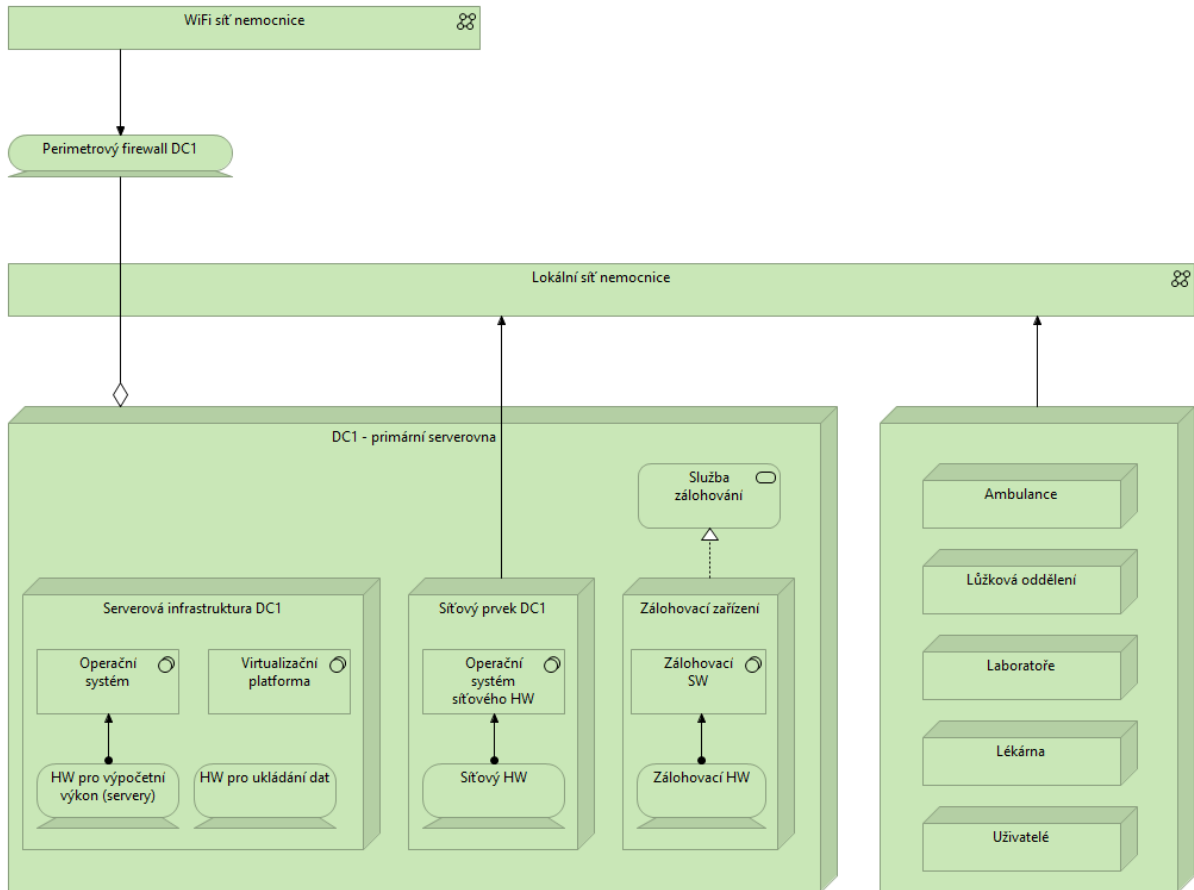
Aktuálně provozovaný firewall byl zakoupen před mnoha lety v rámci běžného provozu IT technologií nemocnice a neumožňuje žádný monitoring sítě ani nespĺňuje aktuální bezpečnostní standardy NUKIB pro předpokládané užití.

Topologie řešení je navržena tak, aby dodávaný firewall měl síťové rozhraní do všech segmentů vnitřní sítě a ke všem případným linkám internetového poskytovatele.

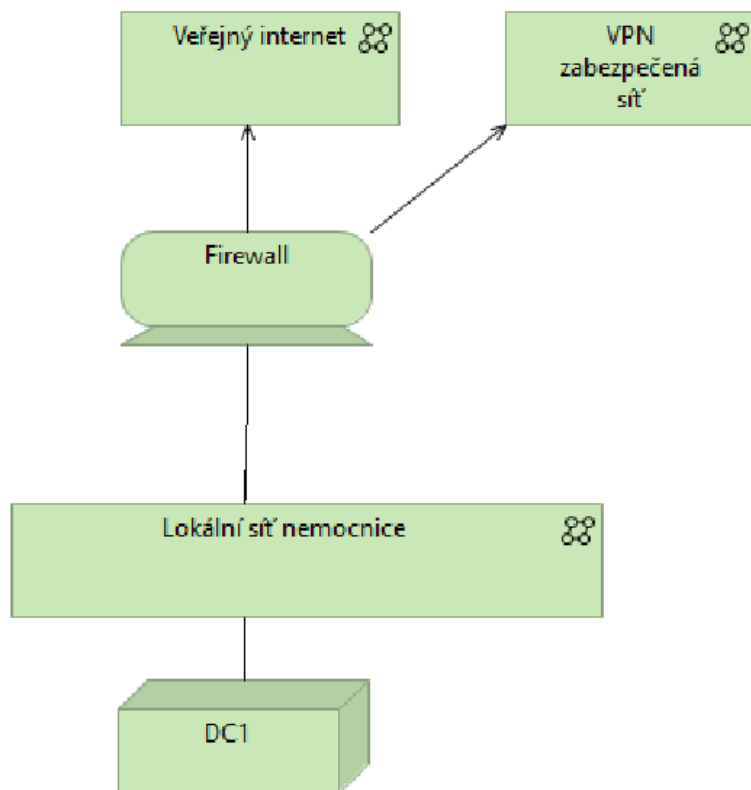
#### Diagram aplikační architektury – pohled struktury aplikací



## Diagram technologické architektury – pohled struktury IT technologické architektury



## Diagram technologické architektury – pohled struktury komunikační infrastruktury



### Rozšíření funkcí o řešení pro emulaci bezpečnostních hrozeb - *požadované technické parametry*

Objednatel požaduje technické řešení zahrnující hardware a software pro zajištění emulace a extrakce bezpečnostních hrozeb. Hlavní bezpečnostní hrozbu objednatel identifikuje ve škodlivém software neznámého původu. Objednatel je v rámci realizace projektu nucen komunikovat na datové úrovni s třetími stranami, kde nemá žádné záruky o původu přiložených dokumentů. Dokument obsahující škodlivý software je pro objednatele nežádoucí, ale jeho obsahová hodnota přesto musí být doručena příjemci (uživatel v rámci infrastruktury objednatele).

### Princip fungování:

1. Nejprve dojde k přijetí potenciálně škodlivého obsahu pomocí stávajících bezpečnostních bran
2. Následně brány zašlou potenciálně škodlivý obsah k inspekci do emulační brány
3. Emulační brána provede analýzu obsahu s cílem odhalit potenciálně škodlivý software
4. Za předpokladu, že software je shledán škodlivým provede emulační brána extrakci škodlivého software
5. Zprávu už bez škodlivého obsahu bezpečnostní brána anebo emulační brána pak doručí požadovanému příjemci. Doručení musí být provedeno takovou formou, která minimalizuje možnost, že škodlivý kód v dokumentu přetrvá. Například u MS Office přílohy dojde k odstranění hrozby a data jsou doručena jako PDF.

Emulaci musí být možné provést na různých operačních systémech dle technické specifikace objednatele. Objednatel vylučuje možnost, že by emulace byla provedena přímo na bezpečnostní bráně. Hlavním důvodem pro toto rozhodnutí je časté užití x86 procesorů v bezpečnostních branách a možné šíření nákazy

pomocí zranitelností vyplývajících z bezpečnostní chyby Spectre a Meltdown. Primárním místem pro emulaci musí být emulační brána. Objednatel připouští, že emulační brána nemusí mít dostatečný výkon k provedení všech požadovaných emulačních procesů. Proto požaduje pouze omezené řešení v technické specifikaci a připouští použití veřejného cloudu výrobce. Avšak brána musí umožnit objednateli rozhodnout, zda-li veřejný cloud bude či nebude použit. Veřejný cloud je zde hlavně pro doplnění potřebného výkonu pro složitější emulaci, nicméně není možné emulační bránu jako celek poskytnout pomocí veřejného cloudu. Takový postup je neakceptovatelný z důvodu ochrany osobních údajů. Objednatel vždy požaduje mít možnost rozhodnout formou konfigurace o tom, že veřejný cloud použit nebude.

Základní množina funkcí: (řešení bude splňovat anebo poskytovat tyto služby)

1. Řešení musí umožňovat emulaci síťového provozu.
2. Emulaci musí být možné provádět ve veřejném cloudu i privátním prostředí objednatele.
3. Řešení musí mít popsané integrační API.
4. Objednatel požaduje možnost nasazení v režimu TAP-SPAN.
5. Řešení nemůže požadovat separátní mailovou infrastrukturu, ale musí takové řešení umožňovat. Tak aby nedocházelo k dalšímu omezení objednatele v oblasti architektury mailového systému.
6. Dynamická analýza souborů a dokumentů na detekci kybernetických hrozeb ve virtuálním prostředí (sandboxing).
7. Ochrana proti technikám obcházení detekce emulace integrovaná přímo v řešení emulační brány.
8. Možnost proaktivní ochrany formou očištění souborů typu MS Office a Adobe PDF od potenciálně nebezpečných komponent, nebo jejich konverze do PDF v průběhu kompletní analýzy v prostředí sandbox pro rychlejší doručení obsahu.
9. Zabezpečení dynamické analýzy proti útokům na různé verze operačního systému:
  - 9.1. Windows XP
  - 9.2. Windows 7
  - 9.3. Windows 8.1
  - 9.4. Windows 10
10. Zabezpečení dynamické analýzy proti útokům na neznámější aplikace:
  - 10.1. Microsoft Office 2003, 2007, 2010, 2013
  - 10.2. Adobe Reader 9, 11
11. Zabezpečení dynamickou analýzu s podporou následujících protokolů:
  - 11.1. HTTP
  - 11.2. HTTPs (dekrypce SSL provozu)
  - 11.3. SMTP, s podporou MTA agenta
  - 11.4. SMTPs (dekrypce TLS provozu), s podporou MTA agenta
12. Možnost aktivní blokáce útoku při první identifikaci hrozby v sandbox prostředí.
13. Možnost manuálního nahrání souborů přímo na emulation appliance přes CLI rozhraní.
14. Monitorování chování spuštěného souboru se zaměřením na změny v systému souborů, systémových registrů, procesů a navázání síťových spojení.
15. Analýza souborů uvnitř SSL a TLS komunikace.
16. Prevence proti vnášení nežádoucích souborů do organizace, možnost vložení do karantény.
17. Monitorování emailové komunikace s kontrolou příloh.
18. Zabezpečení aktualizace signatur pro již známé soubory.
19. Tvorba vlastních signatur.
20. Konfigurační možnosti:
  - 20.1. Granulární definice politik – per IP adresa/síť
  - 20.2. Granulární definice politik – per uživatelská identita
  - 20.3. Výjimky v definici politik – per IP adresa/síť/uživatel
  - 20.4. Výjimky v definici email politik – per odesílatel/příjemce/doména
  - 20.5. Výjimky v definici politik – per soubor (MD5)
21. Tvorba přehledných reportů:
  - 21.1. Detailní analýza všech aktivit (zápisy do registrů, změny ve filesystem, síťové spojení, analýza systémových procesů)
  - 21.2. Detailní popis všech volání procesů
  - 21.3. Export reportu do PDF

22. Řešení musí zpracovávat tyto typy souborů: 7z cab csv doc docm docx dot dotm dotx exe jar pdf potx pps ppsm ppsx ppt pptm pptx rar rtf scr swf tar xla xls xlsb xlsx xlt xltm xltx xlw zip zip com gz bz2 tgz ISO js cpl vbs jse vba vbe wsf wsh. Objednatel vyžaduje z možností identifikace těchto souborů na aktuálních bránách Check Point 4800.
23. Emulace musí podporovat soubory alespoň s velikostí 10MB.
24. Řešení musí splňovat základní principy strojového učení a tato metoda musí být použita pro další vyhodnocování.
25. Řešení musí obsahovat analýzu:
  - 25.1. E-mailového provozu
  - 25.2. Command and Control komunikace
  - 25.3. URL obsažených v dokumentech
26. Analýza musí být prováděna také s ohledem na identifikaci škodlivých stránek, adresních rozsahů na základě reputační databáze.
27. Řešení musí v rámci emulace identifikovat alespoň tyto procesy:
  - 27.1. Volání API
  - 27.2. Změny souborového systému
  - 27.3. Změny v registrech
  - 27.4. Síťová spojení
  - 27.5. Systémové procesy
  - 27.6. Přístup k souborovému systému (čtení, psaní, spouštění a modifikaci)
  - 27.7. Manipulaci s Kernel code:
    - 27.7.1. Chování Kernel code
    - 27.7.2. Přímé interakce CPU
    - 27.7.3. Detekce obfuskačních pokusů
28. Pokusy o útok typu privilege escalation

Základní množina hardware vlastností:

29. Počet instancí unikátního souboru, jež dokáže appliance v rámci jedné hodiny: 1000
30. Prostupnost na aplikační vrstvě: 600 Mbps
31. Počet rozhraní pro komunikaci: 4 x 1 GbE (RJ-45 nebo metalické SFP)
32. Počet rozhraní pro out of band management: 2 x 1 GbE (RJ-45 nebo metalické SFP)
33. Možnost o rozšíření o další porty: 4 x GbE nebo 2 x 10 GbE (v závislosti na volbě modulu, obě možnosti musí být podporovány)
34. Rozměry: Maximálně 2 RU (umístěno do racku o maximální hloubce 800 mm)
35. Napájecí PSU: 2 x redundantní 1+1 AC

### ***Přesun funkce smart event a smart log do virtuálního prostředí OBJEDNATELE***

Vzhledem k očekávanému nárůstu logů (také z emulační brány) požaduje objednatel přesun funkce Check Point Smart Event a Check Point Smart Log z aktuální hardware appliance do virtuálního prostředí. Tato operace by měla proběhnout v rámci nasazení řešení pro emulaci bezpečnostních hrozeb. Dodavatel je povinen dodat potřebné licence na tuto funkci. Nová virtuální platforma by měla být schopna pokrýt potřeby do budoucna, a to nejméně pro sběr událostí z 2 bran. Platforma bude umístěna v privátním cloudu objednatel. Veřejný cloud není přípustný.

### ***Sběr a uchování provozních logů***

Důvody, které zdůvodňují pořízení a nasazení takového systému jsou zejména

- centrální úložiště logů infrastruktury Nemocnice Kadaň
- centrální přehled o infrastruktuře s dashboardy pro IT pracovníky
- forenzní analýza a rychlé vyhledávání v uložených záznamech
- korelace událostí



- alerting a reporting
- sjednocení formátu logů
- uchování a uložení události v jejím RAW formátu
- dlouhodobé uložení
  - plní požadavky Zákona o kybernetické bezpečnosti a ČSN ISO 27001 pro pořizování auditních záznamů
  - uchování logů pro předložení organizacím zabývajících se bezpečností CESNET CERST a CIRST nebo Policii ČR
  - ukládání logů ze všech síťových a bezpečnostních zařízení, serverů, případně stanic
- předcházení ztrátě kritických dat – ochrana proti běžné praxi kybernetických útočníků – zahlazování stop. Při každém úspěšném proniknutí do systému útočník v první řadě maže nebo modifikuje všechny logy a tím pádem i důkazy o kompromitaci systému. Přeposláním logů v reálném čase na centrální úložiště získáte jistotu nemodifikovaných dat, díky kterým můžete nalézt nejen, že byl systém kompromitován, ale hlavně jakým způsobem útočník do systému pronikl. Bez zjištění kudy útočník do systému pronikl, totiž není možné systém zabezpečit proti opakovanému útoku.
- sběr logů pro řešení provozních problémů a bezpečnostních incidentů
- intuitivní a rychlé vyhledávací rozhraní
- ověření přijetí záznamu do úložiště (pokud je podporováno odesílajícím zařízením)
- ověření identity zdroje záznamů, aby nemohl být záznam podvržen (pokud je podporováno odesílajícím zařízením)

Předmětem nasazení bude centrální úložiště logů pro sběr bezpečnostních událostí z kritických systémů, serverů a aplikací.

Nutností je možnost procházení těchto logů vhodným grafickým nástrojem s před-definovanými pravidly pro rychlé vyhledávání (například jako jsou změny v systémech provedené administrátory, seznam nově vytvořených účtů v MS AD za zvolenou periodu, změny v přístupových právech pro zadaného uživatele nebo k zadané složce a monitoring privilegovaných účtů, sdílených účtů a změn konfigurací apod.)

Cílem je mít jednotné úložiště logů, ke kterému budou mít přístup pouze autorizovaní pracovníci objednatel. Nutností je vyloučit možnost modifikace logů ze strany administrátorů nebo uživatelů.

Systém musí umožňovat tvorbu uživatelsky definovaných parserů bez účasti výrobce nebo dodavatele a dokumentace v českém jazyce musí poskytnout jednoznačný návod, jak takovéto parsery vytvářet.

### **Doplňkové vlastnosti firewallu**

- SPI stateful packet inspection: klasický firewall na 4. vrstvě - sleduje relace procházejících síťových připojení a umožňuje průchod paketů, které jsou odpovědí na požadavky, vyvolané zevnitř sítě.
- GeolP blokáce: GeolP filtrování může blokovat webový provoz z celých zemí, což je jeden z mechanismů, jak zabránit hackerům v útoku na vaši firmu. Síťová připojení jsou blokována na základě zeměpisné polohy (informace získané z IP adres), kterou lze následně použít k filtrování a zabránění odchozím a příchozím připojením do vaší firmy a z ní. Seznamy IP adres jsou výrobcem pravidelně aktualizovány a automaticky stahovány do zařízení.
- Anti-Spoofing: detekuje pakety s falešnými zdrojovými adresami a blokuje je.
- Captive Portal: autentizace nových uživatelů LAN sítě (libovolno jestli bezdrátové nebo drátové) před přidělením přístupu do interní sítě.
- Pravidla založená na čase: umožňuje aktivaci pravidel brány firewall v zadaných dnech a/nebo časových rozmezích. Pravidla založená na čase fungují stejně jako jakákoli jiná pravidla s tím rozdílem, že mimo naplánovaný čas nejsou aktivní.

- DoS ochrana: blokuje příchozí provoz, který překračuje nastavené limity a tím zabraňuje zahlcení firewallu při potenciálním DoS útoku.
- DoS ochrana: blokuje příchozí provoz, který překračuje nastavené limity a tím zabraňuje zahlcení firewallu při potenciálním DoS útoku.
- DoS ochrana: blokuje příchozí provoz, který překračuje nastavené limity a tím zabraňuje zahlcení firewallu při potenciálním DoS útoku.
- Routing: Směrování založené na zásadách předává a směruje datové pakety na základě zadaných zásad nebo filtrů s použitím parametrů, jako je zdrojová a cílová IP adresa, zdrojový nebo cílový port, typ provozu, protokoly, seznam přístupů, velikost paketů atd., a pak směruje pakety po uživatelsky definovaných trasách.
- IPv4 / IPv6: mapování NAT pro příchozí a odchozí provoz podporuje souběžně IPv4 a IPv6, což usnadní konfiguraci statických tras na směrovači.
- Statické směrování: plná podpora, včetně nastavitelných priorit
- IPv6 network prefix translation
- DoS ochrana: blokuje příchozí provoz, který překračuje nastavené limity a tím zabraňuje zahlcení firewallu při potenciálním DoS útoku.
- Možnost provozu více IP adres na jednom rozhraní
- Podpora multi-WAN pro loadbalancing a failover
- Podpora obvyklých dynamických routovacích protokolů (BGP, OSPF, RIP)
- IDS/IPS: Systémy detekce narušení (IDS) analyzují síťový provoz a hledají signatury, které odpovídají známým kybernetickým útokům. Systémy prevence narušení (IPS) také analyzují pakety, ale mohou také zastavit jejich doručení a pomoci tak zastavit útok.
- Paketová kontrola: paketový sniffer monitorující síťový provoz v reálném čase. Každý paket je pečlivě zkoumán, aby systém odhalil nebezpečné užitečné zatížení nebo podezřelé anomálie.
- Detekce na 7 vrstvě: Vrstva 7 je aplikační vrstva dle modelu OSI (Open System Interconnection), podporuje procesy aplikací a koncových uživatelů, například HTTP a SMTP. Útoky na této vrstvě představují bezpečnostní problém, protože škodlivý kód se může maskovat jako platné požadavky klienta a běžná data aplikace.
- Databáze hrozeb: systém IDS/IPS lze nakonfigurovat tak, aby detekované síťové události pouze zaznamenávalo, nebo aby je zaznamenávalo i blokovalo. Databáze signatur různých útoků a zranitelností je výrobcem neustále aktualizována a v rámci jeho cloudové služby je automaticky stahována do zařízení. Signatura nově zjištěné kybernetické hrozby může být v zařízení již do 1 hodiny od zveřejnění.
- DoS ochrana: blokuje příchozí provoz, který překračuje nastavené limity a tím zabraňuje zahlcení firewallu při potenciálním DoS útoku.
- IPsec: IPsec je skupina protokolů, které se společně používají k vytvoření šifrovaných připojení mezi zařízeními. Pomáhá zabezpečit data přenášená přes veřejné sítě. IPsec se používá zpravidla pro stabilní VPN tunely typu site-to-site. Touto cestou je možné vytvořit permanentní zabezpečené propojení s pobočkami. IPsec je rovněž podporován většinou síťových zařízení ostatních výrobců.
- SSL VPN : typicky se používá pro vzdálené připojení firemních uživatelů, protože díky použitému protokolu, který je šifrován dnes běžně používaným moderním mechanismem TLS, je tato služba kompatibilní prakticky s jakoukoliv sítí, ve které se uživatel může nacházet, včetně sítí s omezeným přístupem (hotely, letiště, apod.).
- DoS ochrana: blokuje příchozí provoz, který překračuje nastavené limity a tím zabraňuje zahlcení firewallu při potenciálním DoS útoku.
- Autentizace: podporovaná je jak autentizace přes MS AD, LDAP a RADIUS server tak lokální autorizace proti VPN serveru.
- Celková propustnost nabízeného řešení je pro IPsec VPN je 13 Gbps a pro SSL VPN 2 Gbps.

- HTTP a HTTPS proxy
- Transparentní proxy a podpora non-transparent proxy
- Filtrování URL a domén
- Filtrování domén a URL: cloudová služba výrobce poskytuje neustále aktualizované seznamy veřejných URL, rozdělených do kategorií. Tyto kategorie je následně možné využívat při definici pravidel webového filtru. Je rovněž možné lokální přeřazení URL do jiné kategorie (pokud byla výrobcem stanovena nesprávně), případně lze vytvářet kategorie vlastní.
- Antivirus: funkce antiviru kontroluje procházející provoz na známé viry. Virové signatury jsou rovněž automaticky aktualizovány pomocí cloudové služby.
- Antivirové proxy servery se chovají jako tradiční webové proxy servery, pouze skenují veškerý obsah procházející přes proxy server na přítomnost virů nebo signatur malwaru. Pokud proxy server identifikuje obsah jako škodlivý, stahování bude zablokováno a klientský počítač bude přesměrován na chybovou stránku.
- SafeSearch: ochrana před nežádoucími výsledky vyhledávání – podporovány jsou vyhledávače Google, Yandex, Yahoo, MSN, LiveSearch.
- Kontrola šifrovaných protokolů (především HTTPS, ale i SMTPS, IMAPS a FTPS): může pracovat ve dvou režimech: je možné provádět jen kontrolu hlaviček, TLS handshaku a předložených certifikátů, z čehož si firewall může vytvořit jistý, ale nekompletní obrázek o daném typu provozu, nebo lze zapnout hloubkovou kontrolu (deep inspection) a nechat firewall provoz zcela dešifrovat, zkontrolovat a následně jej opět zašifrovat poslat klientovi. Vzhledem k tomu, že v dnešní době je naprostá většina internetového provozu šifrovaná, je toto jediné opravdu účinné řešení plnohodnotné inspekce provozu. Nabízené řešení je vybaveno hardwarovou akcelerací šifrování a dešifrování, díky které je schopno tuto inspekci provádět rychlostí až 4 Gbps.
- Logování přístupu k webovým stránkám
- Domain Name blacklisting
- Reporty: Systém umožňuje sledovat používání internetu. Procházením protokolů o přístupu k proxy serverům lze vytvářet webové přehledy, které podrobně popisují adresy URL, k nimž každý uživatel v síti přistupoval podle data a času, využití šířky pásma a přehledy nejnavštěvovanějších stránek - aniž by o tom uživatelé sítě věděli.
- DHCP server + relay
- DNS forwarding
- DNS server
- Konfigurace přes webový prohlížeč, nebo příkazový řádek
- Sada předdefinovaných wizardů pro konfiguraci systému
- Možnost vzdálené administrace
- Konfigurovatelné přehledové dashboardy
- Nástroje pro snadnou zálohu a obnovu systému
- Jednoduchý systém aktualizací firmwaru
- Možnost automaticky či manuálně vytvářet snímky konfigurace v daném čase s možností zobrazení rozdílů historického snímku oproti aktuálnímu, případně možnost vrácení konfigurace ke zvolenému snímku
- Ověřování proti lokální databázi, MS AD, LDAP a nebo RADIUS serveru.
- Možnost definic skupin uživatelů

- Možnost nasazení Single Sign-On (SSO) mechanismu ve spolupráci s AD, čímž firewall získá informaci o tom, která IP adresa v dané chvíli patří kterému uživateli, což lze použít jak pro logování, tak i pro řízení přístupu uživatelů do sítě např. na bázi členství v AD skupině.
- Možnost dvoufaktorového ověřování VPN klientů.
- podpora high availability clusteringu: podporované režimy active – passive i active – active, synchronizace stavové tabulky firewallu (při failoveru budou služby, postavené na protokolu TCP fungovat beze změny)
- reverzní proxy: nabízí ochranu veřejně publikovaných webových serverů uvnitř sítě, kdy pomocí specializované sady signatur kontroluje provoz z internetu směrem na vnitřní servery a tvoří tak dodatečnou ochrannou vrstvu před samotným webovým serverem.
- Load balancing : navrhované řešení obsahuje poměrně flexibilní loadbalancer, umožňující balancovat protokoly HTTP, HTTPS, TLS/SSL, generický TCP/UDP (L4) a IP (L3) protokol.
- Automatický failover po ztrátě spojení
- Traffic Shapping – prioritizace určitých druhů provozu, možnost selektivního omezení šířky pásma
- Navrhované boxy mají dva nezávislé redundantní napájecí zdroje.
- Customizovatelné dashboardy s přehledy
- Real-time grafy provozu a dalších charakteristik
- SNMP monitoring
- Systém notifikací
- Dostupné API
- Možnost doplnění firewallu o pokročilý nástroj pro sběr a analýzu logů stejného výrobce (virtuální, nebo fyzický box), který se může integrovat přímo do webového rozhraní firewallu.
- Možnost odesílání statistik procházejícího síťového provozu standardními protokoly NetFlow a sFlow.
- Podpora zasílání logů firewallu standardním protokolem SYSLOG.

#### 1.4 Segmentační prvky

V této položce se jedná o přepínače (switche), které umožní oddělení segmentu vnitřní sítě objednatele na část Demilitarizované zóny, v které budou provozovány služby transakčního portálu. Oddělení části sítě je nezbytné z důvodu požadavků a standardů řešení kybernetické bezpečnosti. Dva kusy jsou nutné z důvodu zajištění vysoké dostupnosti služby (v případě poruchy jednoho prvku převezme řízení provozu sítě druhý switch bez dopadu na provoz služeb sítě).

Požadované přepínače HPE FlexNetwork řady 5140 EI obsahují gigabitové ethernetové přepínače, které podporují statické směrování, směrování OSPF a RIP Layer 3, praktické pevné uplinkové porty 10 GbE, PoE+, ACL, IPv6 a přináší úspory energie díky energeticky účinnému ethernetu. Unikátní technologie Intelligent Resilient Fabric (IRF) vytváří virtuální strukturu tím, že spravuje několik přepínačů jako jedno logické zařízení, které zvyšuje odolnost, výkon a dostupnost sítě a zároveň snižuje provozní složitost.

#### Technická specifikace

Jde o gigabitové přepínače, které podporují statické směrování, směrování OSPF a IP Layer 3 směrování. Systém umožňuje vytvořit virtuální strukturu a tím spravovat více přepínačů jako jedno logické zařízení, které zvyšuje odolnost, výkon a dostupnost sítě a zároveň snižuje provozní složitost systému.

#	Parametr	Hodnota
1	Porty, sloty	48x RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only
2	Procesor	256MB Flash 512MB RAM
3	Formát	Montovatelný do 19" RACKu
4	Výkon	1000 Mb Latency < 5 $\mu$ s 10 Gbps Latency < 3 $\mu$ s Throughput 131 Mpps Routing/Switching capacity 176 Gbps Routing table size 1024 entries MAC address table size 16384 entries
5	Pracovní podmínky	Rozsah pracovních teplot: -5°C to 45°C Povolená vlhkost pro provozní podmínky: 10% to 90%, bez kondenzace
6	PoE výkon	370 W PoE+ Automatická detekce zařízení PoE
7	OpenFlow	Podporuje specifikaci OpenFlow 1.3, která umožňuje SDN díky oddělení datových (předávání paketů) a řídicích (rozhodování o směrování) cest.
8	QoS	Umožňuje omezit rychlost vysílání, aby se snížil nežádoucí provoz vysílání v síti. Služba QoS je založená na klasifikátorech – zařízení klasifikuje provoz pomocí více kritérií na základě informací z 2., 3. a 4. vrstvy; aplikuje zásady QoS, jako je nastavení úrovně priority a omezení rychlosti pro vybraný provoz na portu, VLAN nebo celém přepínači. Podporuje následující akce při přetížení: řazení do fronty striktně dle priority (SP), vážené řazení s kruhovou rotací (WRR) a SP+WRR Podpora přístupové rychlosti (CAR) a linkové rychlosti
9	Konektivita	Poskytuje 48 pevných portů 10/100/1000BASE-T v přepínači vrstvy 2/vrstvy 3 Na všech portech podporuje napájení přes Ethernet (PoE+) podle standardu IEEE 802.3at Auto-MDIX - automaticky se přizpůsobí pro přímé nebo křížené kabely na všech portech 10/100/1000 Zajišťuje zpětnou vazbu pomocí standardu IEEE 802.3x, čímž snižuje přetížení v situacích s velkým provozem Umožňuje detekci problémů na vrstvě datového spoje, které se vyskytly v "poslední míli", pomocí standardu IEEE 802.3ah OAM

10	Vysoká dostupnost	<p>Zařízení má redundantní napájení</p> <p>Podporuje Spanning Tree/MSTP, RSTP, PVST+, RPVST+ - redundance spojů s podporou protokolů, jako jsou Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), Per-VLAN Spanning Tree (PVST+), Rapid Per-VLAN Spanning Tree (RPVST+), Equal-Cost Multipath (ECMP) a Smart Link, pro zajištění vysoké dostupnosti.</p> <p>Zařízení podporuje oddělení datových a management cest pro tj. udržuje je odděleně pro zvýšení bezpečnosti a výkonu</p> <p>Zařízení podporuje vytváření virtuálních sítí, kde dva nebo více přepínačů fungují jako jeden přepínač L2 a směrovač L3 přičemž přepínače nemusí být umístěny společně a mohou být součástí DRP;</p> <p>Servery nebo přepínače lze připojit pomocí standardního protokolu LACP pro automatické vyrovnávání zátěže a vysokou dostupnost;</p>
11	Routing na 3 vrstvě	<p>Zařízení podporuje:</p> <p>Statické směrování IP,</p> <p>OSPF s podporou protokolů OSPFv1/v2 a OSPFv3,</p> <p>RIP - podporuje směrování RIPv1 a RIPv2 a obsahuje ochranu proti smyčkám.</p>
12	Správa	<p>Zařízení umožňuje konfiguraci a správu prostřednictvím zabezpečeného webového prohlížeče nebo rozhraní CLI umístěného na vzdáleném zařízení.</p> <p>Poskytuje bezpečné, snadno použitelné grafické rozhraní pro konfiguraci zařízení prostřednictvím protokolu HTTPS</p> <p>Zařízení umí řídit oprávnění tj. umí poskytnout přístup pouze pro čtení (operátor) a čtení/zápis (manažer) a to na rozhraních pro správu CLI a webového prohlížeče.</p> <p>Využívá HWTACACS k propojení vlastního seznamu příkazů CLI s přihlášením jednotlivého správce sítě; poskytuje auditní stopu provedených úkonů.</p> <p>Zařízení provádí kompletní protokolování relací s tím poskytuje podrobné informace pro identifikaci a řešení problémů</p> <p>Používá standardní protokol SNMP k monitorování základních síťových funkcí; podporuje skupiny událostí, alarmů, historie a statistik a privátní skupinu rozšíření alarmů.</p> <p>Plně podporuje IEEE 802.1AB Protokol LLDP (Link Layer Discovery Protocol)</p> <p>Podporuje sFlow (RFC 3176) tj. poskytuje škálovatelné monitorování sítě na bázi ASIC bez dopadu na výkon sítě a umožňuje shromažďovat informace o síti pro účely plánování kapacity a monitorování sítě v reálném čase.</p> <p>Podpora VLAN umožňující segmentovat provoz do a z rozhraní pro správu, včetně rozhraní CLI/telnet, rozhraní webového prohlížeče a SNMP.</p> <p>Umožňuje zrcadlit vstupní provoz vybraný pomocí ACL z portu přepínače nebo VLAN do místního nebo vzdáleného portu přepínače kdekoli v síti.</p> <p>Podpora protokolu DLDP (Device Link Detection Protocol) - monitoruje trasu mezi dvěma kompatibilními přepínači a vypíná porty na obou koncích, pokud je kabel přerušen, což zabraňuje problémům v síti, jako jsou smyčky</p> <p>Správa na úrovni protokolu IPv6 - přepínač lze spravovat bez ohledu na to, zda připojená síť používá protokol IPv4 nebo IPv6; podporuje protokoly pingv6,</p>

		<p>tracertv6, Telnetv6, TFTPv6, DNSv6, syslogv6, FTPv6, SNMPv6, DHCPv6 a RADIUS pro IPv6.</p> <p>Zařízení monitoruje vstupní a výstupní porty a umožňuje řešení problémů v síti a podporuje virtuální testy kabelů,</p> <p>Vestavěný nástroj pro správu sítě s webovým grafickým uživatelským rozhraním, který zjednodušuje provoz a usnadňuje centralizovanou správu. Nástroj umožňuje centralizované zálohování konfigurace, správu verzí softwaru a bezproblémovou výměnu přepínačů.</p> <p>Vestavěný nástroj na identifikaci a správu poruch, konfiguraci prvků a monitorování sítě z centrálního bodu; správce sítě může centrálně spravovat všechny síťové prvky pomocí řady automatizovaných úloh, včetně zjišťování, kategorizace, základních konfigurací a imagů; software rovněž poskytuje nástroje pro porovnávání konfigurací, dohledávání verzí, alertování změn a další</p> <p>Zařízení podporuje SNMP v1/v2c/v3, MIB-II s Traps a RADIUS Authentication Client MIB (RFC 2618); Zařízení obsahuje vestavěný nástroj pro správu HTML se zabezpečeným přístupem.</p>
13	Bezpečnost	<p>Podporuje ACL - poskytuje filtrování provozu na 2. až 4. vrstvě IP; podporuje globální ACL, VLAN ACL, port ACL a IPv6 ACL.</p> <p>Podporuje IEEE 802.1X - standardní metoda ověřování uživatelů pomocí IEEE 802.1X na klientovi ve spojení se serverem RADIUS.</p> <p>Podporuje ověřování na základě MAC, kdy je klient ověřován serverem RADIUS na základě MAC adresy.</p> <p>Podporuje zabezpečení a řízení přístupu založené na identitě</p> <ul style="list-style-type: none"> <li>- Seznamy ACL pro jednotlivé uživatele: povoluje nebo zamítá přístup uživatelů ke konkrétním síťovým prostředkům na základě identity uživatele a denní doby, což umožňuje více typům uživatelů ve stejné síti přistupovat ke konkrétním síťovým službám, aniž by bylo ohroženo zabezpečení sítě nebo hrozil neoprávněný přístup k citlivým datům.</li> <li>- Automatické přiřazování sítí VLAN: automaticky přiřazuje uživatele do příslušné sítě VLAN na základě jejich identity.</li> </ul> <p>Zabezpečený přístup ke správě prvku: Poskytuje bezpečné šifrování všech přístupových metod (CLI, GUI nebo MIB) prostřednictvím SSHv2, SSL, HTTPS a/nebo SNMPv3.</p> <p>Zabezpečené FTP/ SCP: umožňuje zabezpečený přenos souborů do přepínače a z něj; chrání před nežádoucím stažením souboru nebo neoprávněným zkopírováním konfiguračního souboru přepínače.</p> <p>VLAN pro hosty: poskytuje ověřeným klientům prostředí založené na prohlížeči, které je podobné IEEE 802.1X</p> <p>Zabezpečení portů: umožňuje přístup pouze k určeným adresám MAC, které určí správce</p> <p>Izolace portů: zabezpečuje a zvyšuje bezpečnost a zabraňuje útočnickům získat informace o připojených uživateli.</p> <p>Ochrana portu STP BPDU: blokuje datové jednotky protokolu mostu (BPDU) na portech, které nevyžadují BPDU, a zabraňuje tak útokům pomocí falešných BPDU.</p> <p>Ochrana kořenového STP: Chrání kořenový STP před škodlivými útoky nebo chybami v konfiguraci.</p>

		<p>Ochrana DHCP: blokuje pakety DHCP z neautorizovaných serverů DHCP, čímž zabraňuje útokům typu "denial-of-service".</p> <p>Ochrana zdroje IP: pomáhá zabránit útokům na podvržení IP adresy</p> <p>Dynamická ochrana ARP: blokuje broadcasty ARP od neautorizovaných hostitelů, čímž zabraňuje odposlechu nebo krádeži síťových dat.</p> <p>RADIUS/HWTACACS: usnadňuje správu zabezpečení správy přepínače pomocí serveru pro ověřování hesla</p>
14	Výkon	<p>Systém využívá nonblocking architekturu: podporuje až 176 Gb/s a přepínací rychlost s propustností až 130,9 Mpps</p> <p>Hardware-based wire-speed ACL: pomáhá zajistit vysokou úroveň zabezpečení a snadnou správu bez dopadu na výkon sítě díky implementaci ACL založené na TCAM.</p>
15	Konvergence	<p>IEEE 802.1AB Protokol LLDP (Link Layer Discovery Protocol): usnadňuje mapování pomocí aplikací pro správu sítě s automatizovaným protokolem LLDP pro zjišťování zařízení.</p> <p>LLDP-MED: umožňuje automaticky konfigurovat síťová zařízení, včetně IP telefonů podporujících protokol LLDP.</p> <p>Kompatibilita s LLDP-CDP: přijímá a rozpoznává pakety CDP z IP telefonů Cisco pro bezproblémovou funkci</p> <p>Napájení přes Ethernet podle standardu IEEE 802.3at (PoE+): poskytuje až 30 W na port, což umožňuje podporu nejnovějších zařízení podporujících PoE+, jako jsou IP telefony, bezdrátové přístupové body a bezpečnostní kamery, a také jakéhokoli koncového zařízení kompatibilního se standardem IEEE 802.3af;</p> <p>Přidělení výkonu PoE: podporuje více metod (automatickou, třídy IEEE 802.3af, LLDP-MED nebo zadanou uživatelem)</p> <p>Hlasová síť VLAN: automaticky přiřazuje VLAN a priority pro IP telefony, čímž zjednodušuje konfiguraci a údržbu sítě</p> <p>IP multicast snooping (datově řízený IGMP): automaticky zabraňuje zahlcení přenosy IP multicast</p>
16	L2 Switching	<p>Zařízení podporuje:</p> <p>16K tabulku MAC adres</p> <p>VLAN tagy: podpora standardu IEEE 802.1Q s 4 094 současnými ID VLAN</p> <p>IEEE 802.1ad QinQ a selektivní QinQ</p> <p>Agregace 10GbE portů: umožňuje seskupení portů pro zvýšení celkové propustnosti dat do vzdáleného zařízení</p> <p>Protokol DLDP (Device Link Detection Protocol): monitoruje propojení linek a vypíná porty na obou koncích, pokud je zjištěn jednosměrný provoz, čímž zabraňuje vzniku smyček v sítích založených na STP</p> <p>Jumbo Frame: zlepšuje výkon velkých datových přenosů; podporuje rámce o velikosti až 9 Kb.</p>
17	L3 Switching	<p>Zařízení podporuje:</p> <p>Protokol ARP (Address Resolution Protocol): určuje MAC adresu jiného IP hostitele ve stejné podsíti; podporuje statické ARP; ARP umožňuje detekci</p>



	<p>duplicitních IP adres; proxy ARP umožňuje normální provoz ARP mezi podsítěmi nebo v případě, že jsou podsítě odděleny na 2. vrstvě sítě.</p> <p>Protokol DHCP (Dynamic Host Configuration Protocol): zjednodušuje správu rozsáhlých IP sítí; podporuje klienta; DHCP Relay umožňuje provoz DHCP mezi podsítěmi.</p> <p>Adresa rozhraní zpětné smyčky: definuje adresu, která je vždy dosažitelná, čímž zlepšuje diagnostické možnosti.</p> <p>Pomocná funkce protokolu UDP (User Datagram Protocol): umožňuje směrovat UDP provoz přes rozhraní směrovače na konkrétní adresy IP unicast nebo subnet broadcast a zabraňuje podvržení serveru pro služby UDP, jako je DHCP.</p> <p>Mapy tras: poskytuje větší kontrolu při redistribuci tras; umožňuje filtrování a změnu metrik tras</p> <p>Server DHCP</p>
--	--

## 1.5 Popis navrhovaného konceptu řešení infrastruktury PORTÁLU

Základem pro běh aplikací je fyzický server, postavený na velmi osvědčené platformě Dell PE R450. Tento server je virtualizován na virtualizační platformě VMware, která je dnes defacto nepsaným standardem na poli virtualizací. Na serveru je nainstalován hypervisor VMware, v jehož režii probíhá spuštění a provoz jednotlivých operačních systémů.

Data jednotlivých operačních systémů i aplikací jsou uložena na samostatném diskovém poli Dell ME 5024 SAS, ke kterému jsou hypervisory připojeny přes SAS 12Gb/s, a to v duálním režimu na primární i záložní kontrolér najednou. Jednotlivá data a jejich přístup k nim je tedy zajištěn proti výpadkům jak z pohledu přístupu k serverům (duplicitní spojení, ochrana proti výpadku komunikace, SAS propojení atd.), tak proti výpadku kontroléru, zároveň i proti výpadku napájení (dvojitý napájecí subsytém), a pochopitelně i proti chybě jednotlivých disků (RAID pole s automatickým přiřazováním SPARE disku). Diskové pole poskytuje prostor pro data se zvýšenými nároky na výkon vstupně/výstupních operací a je All-Flash.

Proti krátkodobým výpadkům elektrického napájení jsou servery připojeny do el. sítě prostřednictvím UPS, osazené management kartou, která zajistí korektní sjetí virtuálních strojů.

## 1.6 Dodávaný HW

Stručný popis HW serveru:

CPU: 2x Intel® Xeon® Gold 5315Y 3.2G, 8C/16T, 11.2GT/s, 12M Cache, Turbo, HT (140W) DDR4-2933

RAM: 512GB (8x 64GB RDIMM, 3200MT/s, Dual Rank, 16Gb)

HDD: 2x 480GB SSD SATA Read Intensive 6Gbps 512 2.5in Hot-plug AG Drive, 1 DWPD

**PowerEdge R450**

## Komponenty

1	PowerEdge R450 Server
1	2.5" Chassis with up to 8 Hard Drives (SAS/SATA) 2 CPU
1	Trusted Platform Module 2.0 V3
2	Intel® Xeon® Gold 5315Y 3.2G, 8C/16T, 11.2GT/s, 12M Cache, Turbo, HT (140W) DDR4-2933
1	Performance Optimized
1	3200MT/s RDIMMs
8	64GB RDIMM, 3200MT/s, Dual Rank, 16Gb
1	Front PERC H745 Front Load
2	480GB SSD SATA Read Intensive 6Gbps 512 2.5in Hot-plug AG Drive, 1 DWPD
1	Dual, Hot-plug, Power Supply Fault Tolerant Redundant (1+1), 800W, Mixed Mode
1	PowerEdge R450 Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM
1	Broadcom 57412 Dual Port 10GbE SFP+, OCP NIC 3.0
1	Broadcom 5719 Quad Port 1GbE BASE-T Adapter, PCIe Low Profile
1	HBA355e Adapter FH & LP, DIB
1	iDRAC9, Enterprise 15G

## Služby

1	ProSupport and Next Business Day Onsite Service, 24 Month(s)
---	--

Název	Počet
DELL PowerEdge R450	2

Záruka: ProSupport and Next Business Day Onsite Service 24 měsíců

Server má v konfiguraci 520GB RAM paměti, kterou lze dále rozšiřovat až do celkové kapacity 1TB.

## Diskové pole Dell ME5024

### Komponenty

1	Dell ME5024 Storage Array
1	ME5024,SHIPPING,EMEA2
1	12Gb SAS 8 Port Dual Controller
2	12Gb HD Mini-SAS to HD Mini-SAS 2M Cable
17	Hard Drive Filler 2.5in, Single Blank
7	3.84TB SSD SAS ISE Read Intensive 12Gbps 512 2.5in Hot-plug AG Drive
1	Rack Rails 2U
1	Power Supply, 580W, Redundant, CE Marking
1	ME Series 2U Bezel
1	European Power Cord 220V

### Služby

1	ProSupport and 4Hr Mission Critical, 24 Month(s)
---	--

Název	Počet
DELL ME5024	1

Záruka: ProSupport and 4Hr Mission Critical, 24 měsíců

Dodávaná konfigurace diskového pole obsahuje 7x 3,84TB SSD disky, které budou konfigurovány v RAID5 včetně SPARE disku. Diskové pole lze nadále rozšiřovat až na celkových 24 HDD. Další rozšíření lze provádět připojení diskové police.

### 1.7 APC Smart-UPS

Proti krátkodobým výpadkům el. napájení jsou servery připojeny do el. sítě prostřednictvím UPS, osazených management kartou, která zajistí korektní sjetí virtuálních strojů. UPS jsou vybaveny management kartou, aby bylo zajištěno korektní sjetí celé infrastruktury.

Popis položky	Množství	mj
---------------	----------	----

<b>Materiál</b>		
záložní zařízení UPS, 5000VA/kW, on-line VFI, záloha 8-60min, 1/1f	3	ks
Paralelní karta do zdířky USSD; limit: 3 paralelní USSD	3	ks
Karta SNMP Ethernet do zdířky UPS, 4GB	3	ks
Nastavitelné 19" rackové lišty pro UPS dual rozšiřitelné ze 48 na 82 cm, vhodné pro UPS od 2U (HE), max. nosnost 50 kg	3	ks
<b>Montáž</b>		
Kompletní nastavení zařízení vč. základní zkoušky zařízení před instalací	3	ks
Montáž záložní zařízení UPS	3	ks
Implementace UPS zařízení do stávajícího monitorovacího systému	9	HZs
Komplexní funkční zkouška UPS zařízení vč. zkušebního provozu a monitoringu	4	HZs
Doprava, školení a ostatní VRN	1	kpl

Název	Počet
APC Smart-UPS 2200VA LCD RM 2U 230V with Smart Connect	1

Záruka: 24 měsíců

## 1.8 Software

Pro provoz celé serverové infrastruktury je nutné tuto pokrýt potřebnými softwarovými licencemi. Seznam a počet potřebných licencí je uveden níže:

### SW licence

1x CSP Windows Server 2022 Datacenter - 16 Core (umožní instalovat potřebný počet virtuálních serverů na fyzický stroj)

2x CSP Windows Server 2022 - 1 Device CAL

1x CSP Windows Server 2022 External Connector (pokrývá licenčně přístup externích uživatelů z internetu)

2x MS SQL Server 2019 Std 2Lic CoreLic – licence pro 4 vCore

## 1.9 Instalační a konfigurační práce HW

Konfigurace HW a instalace aktuálních firmware

Instalace a konfigurace virtuálního prostředí

Instalace MS Windows serveru (instalace a konfigurace OS, instalace oprav)

Instalace databázového prostředí

Implementace techniky u zákazníka

Příloha č. 2 – Položkový rozpočet

Položky	Počet	Cena za ks bez DPH [Kč]	Cena za ks s DPH [Kč]	Cena celkem bez DPH [Kč]	Cena celkem včetně DPH [Kč]
Firewall	1	4 010 000,00	4 852 100,00	4 010 000,00	4 852 100,00
Segmentační prvky	2	183 920,00	222 543,20	367 840,00	445 086,40
Disková pole, 2x server, web server MS SQL	1	2 240 000,00	2 710 400,00	2 240 000,00	2 710 400,00
Transakční datový portál - komunikace s pacientem - licence	1	940 000,00	1 137 400,00	940 000,00	1 137 400,00
Trans. datový portál - rozšiřující moduly a funkce	1	400 000,00	484 000,00	400 000,00	484 000,00
Trans. datový portál - implementace, napojení na NIS, LIS, PACS	1	720 000,00	871 200,00	720 000,00	871 200,00
Trans. datový portál - NIA a infomované souhlasy	1	210 000,00	254 100,00	210 000,00	254 100,00
Trans. datový portál - napojení na datové komunikační centrum a NCP	1	550 000,00	665 500,00	550 000,00	665 500,00
Rozšíření konektoru pro datovou výměnu s Krajským komunikačním centrem a ZZS	1	240 000,00	290 400,00	240 000,00	290 400,00
UPS serverovna	1	250 000,00	302 500,00	250 000,00	302 500,00
<b>Celkem</b>				<b>9 927 840,00</b>	<b>12 012 686,40</b>

### **PŘÍLOHA Č. 3 SMLOUVY O DÍLO – Podrobný harmonogram** (dále jen „příloha“)

uzavřená ve smyslu ust. § 2586 a násl. a ust. § 1746 zákona č. 89/2012 Sb., občanského zákoníku (dále jen „Občanský zákoník“), ve znění pozdějších předpisů a podle zákona č. 121/2000 Sb. (dále jen „autorský zákon“), ve znění pozdějších předpisů

#### **Objednatel:**

Nemocnice Kadaň s.r.o.

se sídlem: Golovinova 1559, 432 01 Kadaň  
IČ: 25479300  
ID datové schránky: z28pu9r  
jednatel: MUDr. Bc. Petr Hossner, MBA, jednatel  
bankovní spojení: UniCredit Bank Czech Republic and Slovakia, a.s.  
číslo účtu: 155977/2700

#### **Zhotovitel nebo Účastník:**

STAPRO s. r. o.

se sídlem: Pernštýnské náměstí 51, 530 02 Pardubice  
IČ: 13583531  
DIČ: CZ699004728  
za níž jedná: Ing. Leoš Raibr, jednatel společnosti STAPRO s. r. o.  
zapsaná v Obchodním rejstříku vedeném Krajským soudem v Hradci Králové spisová značka C 148  
tel.: +420 467 003 111 fax.: +420 467 003 119, e-mail: obchod@stapro.cz  
bankovní spojení: ČSOB a.s. / Oberbank AG  
číslo účtu: 271810793/0300 / 2171133923/8040  
dále společně jako „smluvní strany“

#### **Etapy**

1. etapa – dodání licencí firewallu, transakčního portálu
2. etapa – dodání hardware, instalace hardware, implementace firewallu
3. etapa – implementace transakčního portálu
4. etapa – podpora dodaného řešení po dobu 5ti let

#### **Termíny**

1. etapa – do 20 pracovních dní od podpisu smlouvy
2. etapa – do 40 pracovních dní od podpisu smlouvy
3. etapa – do 120 pracovních dní od podpisu smlouvy
4. etapa – 60 měsíců od ukončení etapy