EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

STUDIE PROVEDITELNOSTI

Dotační oblast:

IROP 2021 – 27: Kybernetická bezpečnost
Specifický cíl 1.1: Využívání přínosů digitalizace pro občany, podniky, výzkumné organizace a veřejné orgány
Místo realizace: Liberecký kraj, MRR

Název projektu:

Kybernetická bezpečnost pro Nemocnici s poliklinikou Česká Lípa, a.s.

Žadatel o dotaci:

Nemocnice s poliklinikou Česká Lípa, a. s.
Purkyňova 1849, 470 01 Česká Lípa, IČ: 27283518

16.8. 2022
Ve formátu změn k 1.6.2023

OBSAH

1. ÚVODNÍ INFORMACE O ZPRACOVATELI STUDIE PROVEDITELNOSTI

Obchodní jméno, sídlo, IČO a DIČ zpracovatele	Grant Help, s.r.o. Praha 1, Nové Město, Václavské náměstí 828/23 IČ: 27645240 DIČ: CZ27645240
Členové zpracovatelského týmu, jejich role a kontakty	Ing. Jan Pištěk Projektový koordinátor z hlediska dotace Tel.:773 993 907 Email: jan.pistek@granthelp.org Ing. Gabriela Smolíková Manažer projektu z hlediska dotace Tel.: 773 993 908 Email: Gabriela.smolikova@granthelp.org
Datum vypracování	16.8.2022

2. ZÁKLADNÍ INFORMACE O ŽADATELI

Obchodní jméno, sídlo, IČO a DIČ žadatele	Nemocnice s poliklinikou Česká Lípa, a. s. Purkyňova 1849, 470 01 Česká Lípa IČ: 27283518 DIČ: CZ27283518
Jméno, příjmení a kontakt na statutárního zástupce	Ing. Pavel Marek – předseda představenstva, generální ředitel Tel.: +420 487 954 002 Email: pavel.marek@nemcl.cz Jan Mencl, DiS. – místopředseda představenstva, technický a provozní ředitel Tel.: +420 487 954 950 Email: jan.mencl@nemcl.cz Představenstvo jedná jako statutární orgán za společnost. Předseda či místopředseda představenstva jsou oprávněni zastupovat společnost samostatně.
Jméno, příjmení a kontakt na kontaktní osobu pro projekt	Ing. Gabriela Smolíková Tel.: +420 773 993 908 Email: gabriela.smolikova@granthelp.org
Nárok na odpočet DPH na vstupu ve vztahu ke způsobilým výdajům projektu (Ano x Ne)	Ano částečný Žadatel je plátce DPH a má nárok na částečný odpočet DPH ve vztahu k aktivitám projektu: DPH je pro rok 2021 kráceno koeficientem 10%, tj 21% * 0,9% = 18,9% DPH (způsobilý výdaj), 2,1% DPH nezpůsobilý výdaj). Pro rok 2022 uvažováno taktéž s koeficientem ve výši 10%.

3. CHARAKTERISTIKA PROJEKTU A JEHO SOULAD S PROGRAMEM

Název projektu	Kybernetická bezpečnost pro Nemocnici s poliklinikou Česká Lípa, a.s.
Informace o podpořeném zařízení/subjektu (Obchodní jméno, sídlo, IČO)	Nerelevantní, žadatelem je Nemocnice s poliklinikou Česká Lípa, a.s.
Místo realizace projektu	Česká Lípa (Liberecký kraj)
Popis cílů projektu	Cílem projektu je zajištění technických bezpečnostních opatření dle § 5, odst. 3, zákona č. 181/2014 Sb., o kybernetické bezpečnosti v rámci zajištění systému IS Nemocnice s poliklinikou Česká Lípa, a.s. a to od data ukončení realizace projektu (žadatel IS sám vlastní i spravuje/provozuje). Cíle projektu jsou plně v souladu s podporovanými aktivitami výzvy.
Cílové skupiny projektu	○ Občané - koncoví uživatelé nemocnicí poskytovaných služeb. Jedná se zejména o občany města České Lípy, kteří jsou příjemci služeb poskytovaných na úseku ochrany a podpory veřejného zdraví, tedy zejména klienti nemocnice, kteří zdravotních služeb využívají, a na které bude mít vyšší efektivnost a stabilita nemocničních systémů nepřímý pozitivní dopad. Samozřejmě – v případě napadení či jiného incidentu v oblasti kybernetické bezpečnosti – může tento dopad být velmi jednoznačný a v nejhorším možném případě může i ovlivnit kvalitu (např. sdílení zdravotnické dokumentace), rychlost či dostupnost zdravotní péče pro pacienty v Nemocnici s poliklinikou Česká Lípa, a.s. ○ Cizinci – koncoví uživatelé nemocnicí poskytovaných služeb (stejně jako ostatní občané ČR, zejména v případě jejich dlouhodobého pobytu v ČR či náhlých potíží, prevence; nejedná se o např. plastické operace na objednání apod., nemocnice tyto služby neposkytuje). ○ Podnikatelské subjekty – žadatel o dotaci je a.s., tudíž je sám součástí cílové skupiny, jeho zaměstnanci využívají/provozují výstup projektu ke každodenní činnosti, dále subjekty spolupracující se žadatelem v rámci ICT, zaměstnanci podnikatelských subjektů, kterým je poskytována závodní lékařská péče apod. ○ Instituce veřejné správy – předávají/přebírají data z ICT systému. ○ Nestátní neziskové organizace: v rámci závodní lékařské péče, jejich zaměstnanci jako koncoví uživatelé služeb. ○ Výzkumné organizace: v rámci závodní lékařské péče, jejich zaměstnanci jako koncoví uživatelé služeb, v případě potřeby i v rámci výzkumných a vývojových projektů – poskytnutí dat týkajících se ICT systému nemocnice.

Popis vazeb na realizované či plánované projekty	Předkládaný záměr výrazně navazuje na následující projekt aktuálně realizovaný zejména ICT oddělením nemocnice s pomocí EU dotace v rámci IROP: ○ název projektu: Nemocniční informační systém, ○ dotace z operačního programu: 11703 - Integrovaný regionální operační program, ○ obsah projektu: pořízení zcela nového nemocničního informačního systému, a to včetně pořízení nových serverů do hlavní i záložní serverovny z důvodu zajištění dostupnosti a dále výměny přístupových switchů v datových rozvaděčích, ○ maximální částka dotace: 12 735 047,65 Kč. Z hlediska dotačního předkládaný záměr navazuje na dalších 13 projektů realizované žadatelem v rámci dotací EU: ○ Moderní zobrazovací metody a robotizace v Nemocnici s poliklinikou Česká Lípa a.s. (IROP) ○ Modernizace vybavení intenzivní péče v Nemocnici s poliklinikou Česká Lípa a.s. (IROP) ○ Magnetická rezonance v Nemocnici s poliklinikou Česká Lípa a.s. (IROP) ○ Obnova centrálních operačních sálů v Nemocnici s poliklinikou Česká Lípa a.s. (IROP) ○ Laboratorní techniky v Nemocnici s poliklinikou Česká Lípa a.s. (IROP) ○ Obnova lůžkového vybavení v Nemocnici s poliklinikou Česká Lípa a.s. (IROP) ○ Komunikace a mobilita bez bariér (ROP NUTS II Severovýchod) ○ Modernizace centrálních operačních sálů (ROP NUTS II Severovýchod ○ Zlepšení zdravotnické péče v regionu prostřednictvím modernizace rentgenového vybavení NsP Česká Lípa ○ (ROP NUTS II Severovýchod) ○ Iktová jednotka v NsP Česká Lípa, přístrojové vybavení - IC Nemocnice s poliklinikou Česká Lípa, a.s. (IOP) ○ Dokončení zateplení objektů areálu Nemocnice s poliklinikou Česká Lípa a.s. - objekt Patologie (OPŽP) ○ Dokončení zateplení objektů areálu Nemocnice s poliklinikou Česká Lípa a.s. - objekt Jídelna (OPŽP) ○ Dokončení zateplení objektů areálu Nemocnice s poliklinikou Česká Lípa a.s. - objekt Dialýza (OPŽP). Projekt neuvažuje ve střednědobém horizontu s konkrétně navazujícími záměry, neboť jeho realizací budou naplněny požadavky nemocnice na kompletní zajištění ICT systému nemocnice odpovídající současným požadavkům. Do budoucna budou plánovány a realizovány projekty s ohledem na vývoj v ICT oblasti včetně zajištění kybernetické bezpečnosti.

4. PODROBNÝ POPIS PROJEKTU

4.1 Podrobný popis výchozího stavu

Výrazný nárůst používání informačních technologií v současném světě vede na jedné straně k vytvoření informační společnosti, urychlení komunikace a velkému rozvoji služeb a tím celé společnosti, na straně druhé vzrůstá i riziko zneužívání těchto technologií, které má rozsáhlé dopady do činnosti subjektů, které s nimi pracují, a potencionálně může vést ke značným škodám, které mohou ve zdravotnictví znamenat ohrožení života pacientů.

Technologické služby nemocnice, na kterých je přímo závislá poskytovaná zdravotní péče, jsou bohužel nejen technologicky zastaralé, ale není již možné na těchto technologiích zajistit spolehlivou kybernetickou bezpečnost s přihlédnutím na bezpečí pacientů.

Pro nemocnici jsou životně důležité IS provozovány nejen na zastaralém a nevyhovujícím HW, ale také SW. Systémy vyjmenované v příloze jsou z velké části provozovány na operačním systému Windows server 2008.

Informační systémy obsahují mnoho citlivých dat, mnoho dat archivní povahy, která jsou důvodem pro urychlenou potřebu investic do moderní ICT infrastruktury, která je schopná zajistit spolehlivou kybernetickou bezpečnost.

Na začátku roku 2022 čelila nemocnice dvěma kybernetickým útokům, které odhalili většinu slabin jak v oblasti vybavení, tak v oblasti zajištění právě kybernetické bezpečnosti.

Stávající síťová infrastruktura organizace sestává z 56 datových přepínačů různých modelů od různých výrobců (3COM, H3C, Cisco, DELL, HP, NETGEAR, TP-LINK, Alcatel-Lucent) rozmístěných ve 25 datových rozvaděčích včetně 2 serveroven a 60 bezdrátových přístupových bodů různých modelů a výrobců (Ubiquiti, AeroHive). Topologie sítě je částečná dvojitá hvězda s centrálními body v serverovnách. Bezdrátová síť nemá jednotnou centrální správu.

Páteřní vrstva datové sítě sestává z L3 přepínačů Alcatel-Lucent, které jsou v konfiguraci virtuálního chassis s jednotlivými uzly umístěnými v obou serverovnách. Toto řešení s sebou nese jistá omezení v podobě mechanismu virtuálního chassis, kdy všechny přepínače v rámci virtuálního chassis musí běžet na stejné verzi firmware. Aktualizace firmware tedy musí být vždy provedena na uzlech virtuálního chassis, což vyžaduje delší servisní interval a prodlužuje případný výpadek v případě roll-back scénáře. Případná softwarová nebo hardwarová chyba na uzlu typu master ovlivní chování i všech ostatních přepínačů v rámci tohoto virtuálního chassis.

Z pohledu dostupnosti je datová síť náchylná ke vzniku konfiguračních a topologických chyb bez možnosti snadné detekce a nápravy, neboť není k dispozici centralizovaná správa. Zabezpečení přístupu k síti na přístupové vrstvě není v současnosti řešeno. Stávající počítačová síť je rozdělena na logické vrstvě dle umístění přístupových přepínačů v jednotlivých datových rozvaděčů. Směrování mezi jednotlivými L2 segmenty sítě je řešeno páteřním virtuálním chassis. Přístup k jednotlivým segmentům sítě je tedy v rámci organizace zcela otevřený a nejsou aplikována žádná kontrola síťového provozu. Toto zcela znemožňuje detekci anomálií v síťové komunikaci a zabránění neoprávněnému přístupu ke všem klientům připojeným do datové sítě v případě neoprávněného přístupu do kteréhokoliv segmentu sítě.

Žadatel hodlá vyřešit nedostatečné zabezpečení datové sítě její obnovou a to aby byla zajištěna vysoká dostupnost a bezpečnost síťových služeb.

V současnosti zadavatel řeší perimetrovou bezpečnost bránou od výrobce FortiGate. Tento firewall není žádným způsobem redundantní a z hlediska topologie má pouze funkci perimetrového firewallu oddělující interní síť od sítě Internet. Konfiguračně dále kromě síťového firewallu plní navíc funkci VPN brány zajišťující vzdálený přístup uživatelů.

Ochrana na úrovni perimetru aktuálně neodpovídá současným bezpečnostním doporučením a standardům a není zajištěna redundance v případě HW problému. Vnitřní segmentace zcela chybí a interní směrování je zajištěno core částí sítě (core switche). Chybí tedy možnost kontroly interního

provozu a filtrace na úrovni identit. Současné řešení postrádá jakékoliv prvky ochrany proti současným hrozbám.

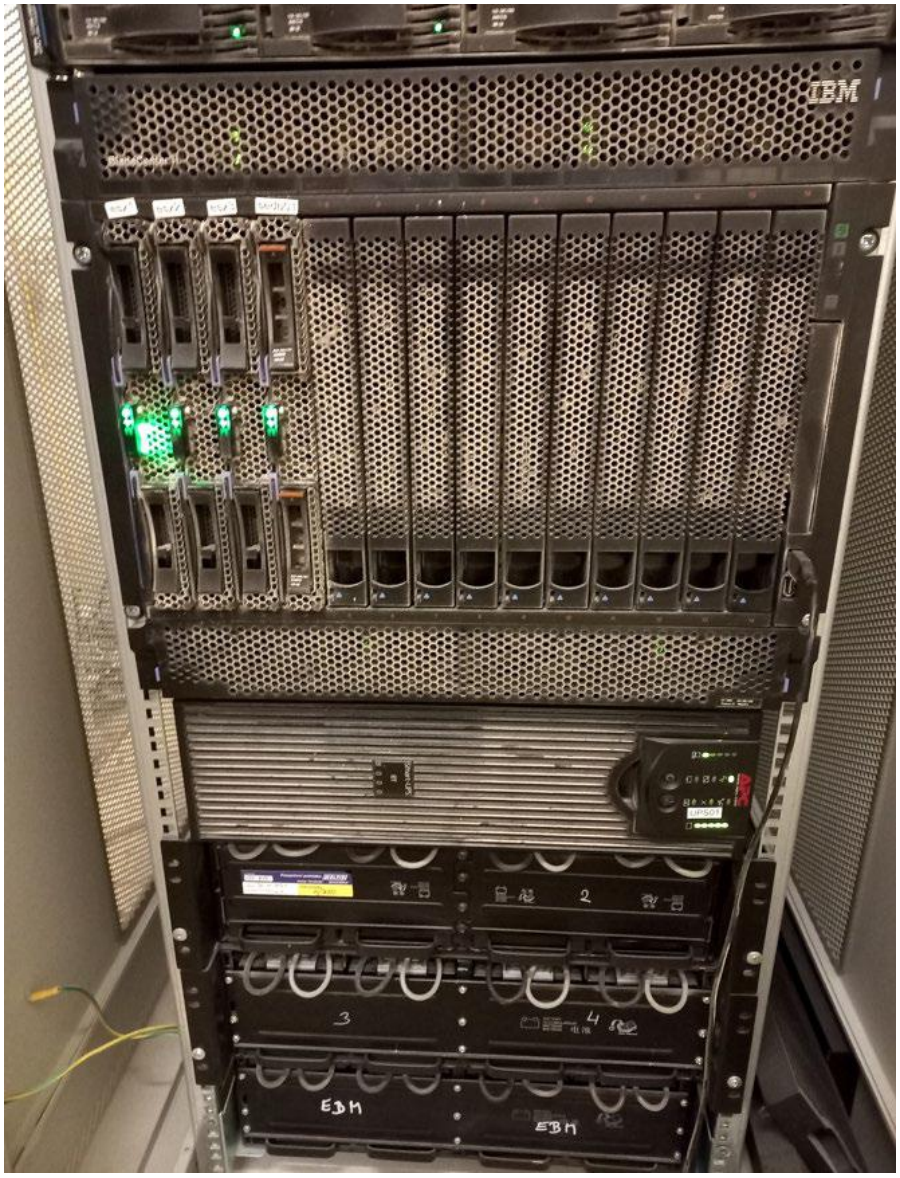
V rámci tohoto projektu je počítáno s nasazením zabezpečení serverovny jak na úrovni místnosti, tak na úrovni rackové skříně s daty. Pro zabezpečení místosti je plánován standardní PZTS systém dle normy ČSN EN 50131-1 ed. 2. Systém bude střežit samotný plášť místnosti (okna, dveře) ale také potenciální pohyb přímo v místnosti, a to pomocí PIR čidel. V případě neoprávněného vstupu dojde k aktivací vnitřní sirény, odeslání zprávy na pult centrální ochrany a také formou SMS na vybrané pracovníky. Do systému budou doplněny i environmentální senzory pro redundantní kontrolu teploty v místnosti (řešeno i v rámci rackové skříně) a také detektory kouře pro případ vzniku požáru

Projekt předpokládá dodání nové záložní výpočetní farmy. Důvodem pro její realizaci je zajištění vysoké dostupnosti výpočetních clusterů. Farma bude postavena pomocí virtualizovaného serverového clusteru s virtualizační technologií VMware vSphere). K farmě budou připojena pro doručení služeb datového úložiště disková pole all-flash. Výpočetní farma bude pracovat v režimu vysoké dostupnosti, i ve vztahu ke stávajícím technologiím na technologii VMware vSphere, které momentálně nejsou redundantní ani v rámci jednoho datového centra – nemají sdílený úložný prostor pro ukládání strukturovaných dat.

Softwarové vybavení NsP, které se neřadí do kategorie běžného osobního použití:

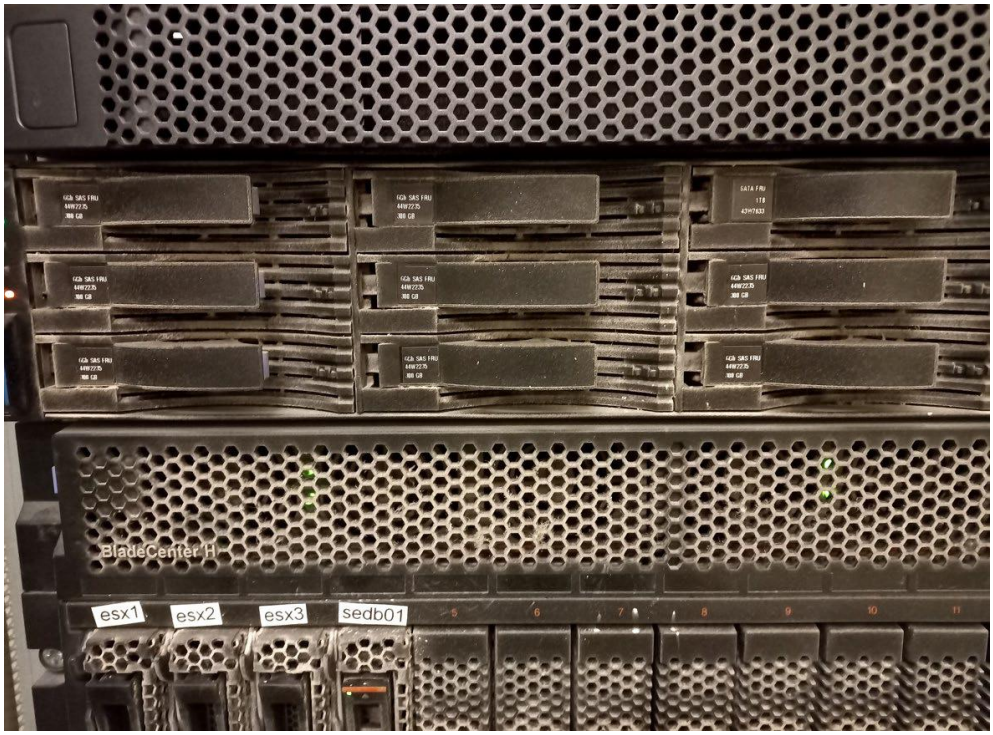
1. IS NIS TREE - informační systém pro Nemocnici
2. Mediox je moderní softwarové řešení, které podporuje všechny klíčové procesy v naší nemocniční lékárně
3. LIMS - řízení laboratoře. Laboratorní Informační a Manažerský Systém, LIMS, slouží k vedení evidencí a řízení procesů v laboratoři.
4. Vema - mzdová a personální agenda
5. NEFRIS - lékařský informační systém pro komplexní vedení zdravotní dokumentace pacientů a vykazování výkonů zdravotním pojišťovnám.
6. Anete Kredit SW – stravovací provoz, bistro
7. PACS - technologie umožňující správu, ukládání (archivaci) a zobrazení obrazové dokumentace (tj. snímků z rentgenových metod, magnetické rezonance, apod.). Jako standard a univerzální formát komprimovaných obrazových dat se používá DICOM (Digital Imaging and Communications in Medicine). PACS sestává ze čtyř komponent: jednak obrazová dokumentace, pak zabezpečená síť, cílové stanice (počítače, terminály) a úložiště dat.

Aktuální stav IBM severů
Nyní na starých serverech běží PACS a databázový server.
Databázový server nese DB pro aplikace LIMS, NEFRIS, ORGIS, DOCTIS, ANETE.
V případě jeho kolapsu dojde k nefunkčnosti těchto aplikací a hrozí ztráta dat.
Fyzicky servery běží na IBM HS-22 Blade Chassi, které bylo v Nemocnici s poliklinikou Česká Lípa instalováno v roce 2010. Tento produkt již od roku 2019 není výrobcem podporován a není možné k němu získat žádné náhradní díly.
Nyní již v Chassi není funkční jeden ventilátor a v případě havárie druhého dojde k automatickému vypnutí celého Chassi a nebude možné jej spustit bez výměny ventilátoru.
Fyzický stav serveru v racku
Aktuálně je celé HW řešení instalováno v Racku. Nachází se v 5. patře polikliniky v místnosti serverovny. Na tomto fyzickém HW nebyla nikdy za dobu jeho provozu provedena pravidelná údržba ani jiná potřebná profylaxe. (šedá barva jsou nánosy prachu, který stabilně zajišťuje přehřívání HW.)


IBM
2
3
4
EJH
EJH

Detailní záběr chassi a jeho vnitřních serverů. Zde jasně ukázáno, že celá serverová struktura běžela v podstatě na jednom fyzickém zařízení, což dle běžných standardů odporuje jak bezpečnostním pravidlům v kybernetické bezpečnosti, tak pravidlům pro zajištění bez výpadkového provozu ICT HW serverové infrastruktury.
Jedná se o kritické úzké hrdlo, při jehož výpadku hrozila nedostupnost všech systémů Nemocnice, potřebných pro chod a zajištění péče pro pacienty.

Datová pole pro IBM chassi
Samotná chassi jsou propojena s několika data storage, jejichž pořízení bylo ve stejném období jako IBM chassi.
Datová



Datová pole jsou stejně jako chassi neudržovaná a vadné HDD nebyly řešeny. Což znamená ztrátu výkonu čtení a zapisu dat.

Síťová architektura IBM chassi

Síť je provozována na 2x BNT Layer 2/3 Copper Gigabit Ethernet Switch Module for IBM BladeCenter. Nyní již také plně bez technické podpory a možnosti zajistit náhradní díly.
V poslední době dochází k výpadkům fyzických portů, jejich přepínání bez zásahu IT oddělení.

Screen ukazuje, že pro zajištění alespoň částečného provozu jsme museli přistoupit k propojení pouze dvěma porty. Při provozu na více portech dochází k výpadkům a celkové nestabilitě celého provozu.
I zde je vidět velký nános prachu.

4.2 Popis jednotlivých částí projektu

4.2.1 Popis částí projektu

a) Výčet informačních a komunikačních systémů, které žadatel spravuje

Předmětem projektu je opatření k zabezpečení IS: NIS TREE, MEDIOX, LIMS, VEMA, NEFRIS, ANETE, PACS, dále kompletní síťová infrastruktura.
Tyto IS nejsou KII/VIS/ISZS. Žadatel je sám vlastníkem i provozovatelem tohoto IS. IS nespravuje jiná organizace. Žadatel nebude zabezpečovat IS pro jinou organizaci.
Projekt předpokládá dodání nové záložní výpočetní farmy. Důvodem pro její realizaci je zajištění vysoké dostupnosti výpočetních clusterů. Farma bude postavena pomocí virtualizovaného serverového clusteru s virtualizační technologií VMware vSphere). K farmě budou připojena pro doručení služeb datového úložiště disková pole all-flash. Výpočetní farma bude pracovat v režimu vysoké dostupnosti, i ve vztahu ke stávajícím technologiím na technologii VMware vSphere, které momentálně nejsou redundantní ani v rámci jednoho datového centra – nemají sdílený úložný prostor pro ukládání strukturovaných dat.

b) Definice a vymezení informačního systému žadatele

Informační systém (IS) v Nemocnice s poliklinikou Česká Lípa, a. s. je komplex lidí, informací, systému řízení chodu IS, který zabezpečuje těsné a logické propojení na prostředí, systému organizace práce spojeného s provozem a využitím IS, technických prostředků a metod zabezpečujících sběr, přenos, aktualizaci, uchování a další zpracování dat pro tvorbu a prezentaci informací pro potřeby uživatelů a použité informační technologie. V prostředí Nemocnice s poliklinikou Česká Lípa, a. s. jde o infrastrukturní HW a dále SW vybavení. U SW vybavení jde o NIS TREE, MEDIOX, LIMS, VEMA, NEFRIS, ANETE, PACS.

4.2.2 Výčet jednotlivých technických opatření podle § 5 odst. 3) zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále "ZKB"), které žadatel plánuje realizovat v rámci projektu

ID opatření:	**1.**
Oblast opatření podle ZKB a vyhlášky o kybernetické bezpečnosti:	*navržená protiopatření splňují požadavky vycházející z Vyhlášky č. 82/2018 Sb, Část druhá, Hlava II a to jmenovitě:* • *§ 18, písm. a) – zajištění segmentace sítě pomocí VLAN tagging (IEEE 802.1Q).* • *§ 18, písm. c) – zajištění důvěrnosti a integrity dat při přenosu dat přes páteřní spoje pomocí šifrovacího protokolu MACsec.* • *§ 19, odstavec 2, písm. a) –autentizace přístupu k administraci páteřních přepínačů pomocí protokolu TACACS+, kdy je kontrolována identita administrátorského uživatele.* • *§ 20, písm. b) – autorizace přístupu k jednotlivým částem operačního systému přepínače a jejich konfiguračních*

	změn prostřednictvím protokolu TACACS+ a to na základě identity a role administrátorského uživatele.
Název opatření:	*Nákup páteřních síťových přepínačů*
KII/VIS/ISZS/IS/KS:	*NIS TREE, MEDIOX, LIMS, VEMA, NEFRIS, ANETE, PACS, dále kompletní síťová infrastruktura.*
Popis opatření:	*Cílem opatření je zlepšit stávající stav síťové infrastruktury organizace se zaměřením na zvýšení dostupnosti a kybernetické bezpečnosti informačních aktiv. Výsledkem bude jednotná infrastruktura na straně datového centra pro připojení serverů, datových úložišť a zálohovacího systému a jednotná infrastruktura na páteřní vrstvě pro připojení přístupových přepínačů*
Sdílení opatření se ISOUI:	*Žadatel neprovozuje ISOUI.*

ID opatření:	**2.**
Oblast opatření podle ZKB a vyhlášky o kybernetické bezpečnosti:	*Navržená protiopatření splňují požadavky vycházející z Vyhlášky č. 82/2018 Sb, Část druhá, Hlava II a to jmenovitě:* • *§ 18, písm. a) – zajištění segmentace sítě pomocí VLAN tagging (IEEE 802.1Q).* • *§ 18, písm. c) – zajištění důvěrnosti a integrity dat při přenosu dat mezi bezdrátovými přístupovými body a centrálním kontrolérem pomocí šifrovaného tunelu pro řídicí i datové toky.* • *§ 19, odstavec 2, písm. a) – autentizace přístupu k administraci centrálního kontroléru i jednotlivých bezdrátových přístupových bodů pomocí protokolu RADIUS, kdy je kontrolována identita administrátorského uživatele.* • *§ 26, písm. a) – použití kryptografických algoritmů dle standardu WPA3-Enterprise, který zároveň zajišťuje generování a distribuci šifrovacích klíčů bezdrátové komunikace a splňuje tak § 26, písm.b) odstavec 1.*
Název opatření:	*Nákup bezdrátových aktivních prvků*
KII/VIS/ISZS/IS/KS:	*NIS TREE, MEDIOX, LIMS, VEMA, NEFRIS, ANETE, PACS, dále kompletní síťová infrastruktura.*

Popis opatření:	*Nedílnou součástí infrastruktury organizace je bezdrátová počítačová síť, která zpřístupňuje služby datové sítě mobilním klientům. Dle současných trendů dochází k pozvolnému přechodu stále většího množství klientů k bezdrátovému připojení a to jak mezi tradičními počítačovými klienty, tak mezi specializovaným vybavením nemocničních areálů. Jedná se o zdravotnická zařízení, která výrobci vybavují bezdrátovými síťovými kartami, aby zjednodušili připojení zařízení do nemocniční infrastruktury, případně zvýšili mobilitu těchto přístrojů. V rámci zkvalitnění poskytované péče a zvýšení komfortu pro své klienty žadatel také plánuje poskytovat přístup k veřejnému internetu i pro pacienty a návštěvníky nemocnice.*
Sdílení opatření se ISOUI:	*Žadatel neprovozuje ISOUI.*

ID opatření:	**3.**
Oblast opatření podle ZKB a vyhlášky o kybernetické bezpečnosti:	*Navrhované řešení centrálního řízení přístupu k síti naplňuje následující body Vyhlášky:* • *§ 19, odstavec 2, písm. a) – systém vystupuje v roli autentizační a autorizačního serveru pro jak řízení přístupu k datové síti, tak pro administrátorský přístup k aktivním síťovým prvkům.* • *§ 19, odstavec 2, písm. b) – systém umožní definovat maximální možný počet neúspěšných pokusů o přihlášení před tím, než bude koncový klient zapsán na seznam blokovaných klientů a bude mu odepřen přístup.* • *§ 19, odstavec 2, písm. c) – systém používá pro autentizaci koncových klientů protokolů, které nepřenášejí privátní hesla nebo klíč přes datovou síť (PEAP-MSCHAPv2, EAP-TLS).* • *§ 19, odstavec 2, písm. e) – Systém umožní nastavení vypršení platnosti přihlášení po uplynutí určitého časového intervalu, během které klient neprovedl reautentizaci. Systém také podporuje rozšíření RADIUS protokolu o funkcionalitu Change-of-Authorization (CoA, RFC 5176), díky které lze vynutit změnu přidělených oprávnění koncovým klientů přímo z centrální systému řízení přístupu. Tímto lze reagovat i na případné změny identity (např. zneplatnění už. certifikátu nebo zamčení už. účtu v ActiveDirectory).* • *§ 19, odstavec 2, písm. g) – systém umožňuje tvorbu pravidel pro správu přístupu jak k drátové a bezdrátové síti, tak i správu administrátorských přístupů k aktivním síťovým prvkům. Je umožněna integrace libovolného koncového*

	autentizačního systému, který podporuje standardní protokoly RADIUS nebo TACACS+. Správa pravidel a identit je prováděna přes jednotné rozhraní systému i v případě, kdy je řešení implementuje dva či více redundantních autentizačních serverů.
Název opatření:	**Centrální řízení přístupu k počítačové síti**
KII/VIS/ISZS/IS/KS:	*NIS TREE, MEDIOX, LIMS, VEMA, NEFRIS, ANETE, PACS, dále kompletní síťová infrastruktura.*
Popis opatření:	*Centrální řízení přístupu k síti předpokládá vytvoření jednotné platformy pro autentizaci a autorizaci přístupu koncových klientů jak k bezdrátové síti tak k drátové síti organizace. Řešení bude založeno na standardních protokolech, aby bylo možno integrovat zařízení různých výrobců a bylo zamezeno závislosti na jednou výrobci.*
Sdílení opatření se ISOUI:	*Žadatel neprovozuje ISOUI.*

ID opatření:	**4.**
Oblast opatření podle ZKB a vyhlášky o kybernetické bezpečnosti:	*navržená protiopatření splňují požadavky vycházející z Vyhlášky č. 82/2018 Sb, Část druhá, Hlava II a to jmenovitě:* • *§ 18, písm. a) – zajištění segmentace sítě pomocí VLAN tagging (IEEE 802.1Q).* • *§ 18, písm. c) – zajištění důvěrnosti a integrity dat při přenosu dat přes páteřní spoje pomocí šifrovacího protokolu MACsec.* • *§ 19, odstavec 2, písm. a) –autentizace přístupu k administraci páteřních přepínačů pomocí protokolu TACACS+, kdy je kontrolována identita administrátorského uživatele.* • *§ 20, písm. b) – autorizace přístupu k jednotlivým částem operačního systému přepínače a jejich konfiguračních změn prostřednictvím protokolu TACACS+ a to na základě identity a role administrátorského uživatele.*
Název opatření:	*Centrální monitoring a správa počítačové sítě*
KII/VIS/ISZS/IS/KS:	*NIS TREE, MEDIOX, LIMS, VEMA, NEFRIS, ANETE, PACS, dále kompletní síťová infrastruktura.*

Popis opatření:	*Rostoucí počet služeb zajišťovaných síťovou infrastrukturou spolu s požadavky na kvalitu a bezpečnost sítě vede ke zvyšování nároku na správu datové sítě. Žadatel v rámci tohoto projektu řeší optimalizaci využití omezených lidských zdrojů na správu infrastruktury. Cílem je dosáhnout optimální míry automatizace pro časté konfigurační úkony a řešení problémů s datovou sítí. Výsledkem je minimalizace rizika vzniku konfiguračních chyb, které mohou představovat bezpečnostní hrozbu, a rychlejší řešení problémů a uvolnění části kapacity IT oddělení na řešení strategických úkolů.* *Základním předpokladem rychlého a účinného řešení problémů síťové infrastruktury je mít aktuální přehled o všech aktivních sítových prvcích společně s možností aktivního zásahu do síťové infrastruktury. Žadatel proto plánuje nasazení centrálního monitorovacího sytému pro aktivní prvky počítačové sítě.*
Sdílení opatření se ISOUI:	*Žadatel neprovozuje ISOUI.*

ID opatření:	**5.**
Oblast opatření podle ZKB a vyhlášky o kybernetické bezpečnosti:	*Řešení z technického pohledu naplňuje dle § 19 odstavce 1 požadavek na zajištění nástroje pro správu a ověření identity aplikací informačního a komunikačního systému. Podle odstavce 2 je nástrojem pro ověření identity aplikací a výpočetních komponent - ověří identitu před zahájením výpočetních aktivit a zajistí centralizovanou správu identit výpočetních systému jako takových.* *Technické řešení současně naplňuje dle § 27 bodu a) až d) požadavek na zajištění:* *dostupnosti informačního a komunikačního systému pro splnění cílů podle § 15,* *odolnosti informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům, které by mohly snížit jeho dostupnost,* *dostupnosti důležitých technických aktiv informačního a komunikačního systému a* *redundance aktiv nezbytných pro zajištění dostupnosti informačního a komunikačního systému.*
Název opatření:	*Zabezpečená výpočetní farma - servery, disková pole, SAN*
KII/VIS/ISZS/IS/KS:	*NIS TREE, MEDIOX, LIMS, VEMA, NEFRIS, ANETE, PACS, dále kompletní síťová infrastruktura.*

Popis opatření:	*Projekt předpokládá dodání nové záložní výpočetní farmy. Důvodem pro její realizaci je zajištění vysoké dostupnosti výpočetních clusterů. Farma bude postavena pomocí virtualizovaného serverového clusteru s virtualizační technologií VMware vSphere). K farmě budou připojena pro doručení služeb datového úložiště disková pole all-flash. Výpočetní farma bude pracovat v režimu vysoké dostupnosti, i ve vztahu ke stávajícím technologiím na technologii VMware vSphere, které momentálně nejsou redundantní ani v rámci jednoho datového centra – nemají sdílený úložný prostor pro ukládání strukturovaných dat.*
Sdílení opatření se ISOUI:	*Žadatel neprovozuje ISOUI.*

ID opatření:	**6.**
Oblast opatření podle ZKB a vyhlášky o kybernetické bezpečnosti:	*Řešení z technického pohledu naplňuje dle § 22 odstavce 1 a 2 požadavek na zajištění nástroje pro zaznamenávání bezpečnostní a potřebné provozní události důležitých aktiv informačního a komunikačního systému.* *Podle odstavce 2 je nástrojem pro sběr informací o bezpečnostních a provozních událostech, před neoprávněným čtením a jakoukoli změnou.* *Technické řešení současně naplňuje dle § 27 bodu b) požadavek na zajištění:* *b. odolnosti informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům, které by mohly snížit jeho dostupnost.*
Název opatření:	*SÍŤOVÁ BEZPEČNOST (OPATŘENÍ PRO REALIZACI CENTRÁLNÍCH FW A CENTRÁLNÍHO LOGSERVERU/ANALYTICKÉHO NÁSTROJE)*
KII/VIS/ISZS/IS/KS:	*NIS TREE, MEDIOX, LIMS, VEMA, NEFRIS, ANETE, PACS, dále kompletní síťová infrastruktura.*
Popis opatření:	*Opatření navrhuje zvýšit jak kybernetickou bezpečnost, tak zajištění vysoké dostupnosti implementací firewall řešení v konfiguraci HA (high availability) clusteru. Jednotlivé prvky firewallu budou fyzicky umístěný již v existujících oddělených DC zadavatele a z pohledu topologie sítě bude firewall připojen k core infrastruktuře. V plném rozsahu bude nahrazen současný hardware a jeho funkcionalitu přebere nové řešení, současně bude pak doplněno o funkcionality nové, a to především:*

	• *Segmentace interní LAN a následná možnost kontroly provozu.* • *Integrace s centrálním zdrojem identit (AD) a kontrola provozu na granulární úrovni.* • *Aktivní ochrana před kybernetickými hrozbami za pomocí modulů IPS, antimalware, antiransomware, AV, antibot apod.* • *Sandboxing technologie doplňující výše jmenované.* • *Implementace logserveru umožňující centrální sběr a analýzu logů.*
Sdílení opatření se ISOUI:	*Žadatel neprovozuje ISOUI.*

ID opatření:	**7.**
Oblast opatření podle ZKB a vyhlášky o kybernetické bezpečnosti:	*Navrhované řešení centrálního řízení přístupu k síti naplňuje následující body Vyhlášky:* • *§ 19, odstavec 2, písm. a) – systém vystupuje v roli autentizační a autorizačního serveru pro jak řízení přístupu k datové síti, tak pro administrátorský přístup k aktivním síťovým prvkům.* • *§ 19, odstavec 2, písm. b) – systém umožní definovat maximální možný počet neúspěšných pokusů o přihlášení před tím, než bude koncový klient zapsán na seznam blokovaných klientů a bude mu odepřen přístup.* • *§ 19, odstavec 2, písm. c) – systém používá pro autentizaci koncových klientů protokolů, které nepřenášejí privátní hesla nebo klíč přes datovou síť (PEAP-MSCHAPv2, EAP-TLS).* • *§ 19, odstavec 2, písm. e) – Systém umožní nastavení vypršení platnosti přihlášení po uplynutí určitého časového intervalu, během které klient neprovedl reautentizaci. Systém také podporuje rozšíření RADIUS protokolu o funkcionalitu Change-of-Authorization (CoA, RFC 5176), díky které lze vynutit změnu přidělených oprávnění koncovým klientů přímo z centrální systému řízení přístupu. Tímto lze reagovat i na případné změny identity (např. zneplatnění už. certifikátu nebo zamčení už. účtu v ActiveDirectory).* • *§ 19, odstavec 2, písm. g) – systém umožňuje tvorbu pravidel pro správu přístupu jak k drátové a bezdrátové síti, tak i správu administrátorských přístupů k aktivním síťovým prvkům. Je umožněna integrace libovolného koncového autentizačního systému, který podporuje standardní protokoly RADIUS nebo TACACS+. Správa pravidel a identit je prováděna přes jednotné*

	rozhraní systému i v případě, kdy je řešení implementuje dva či více redundantních autentizačních serverů. *Návaznost na § 20.* • *písm. a) – řízení přístupu k jednotlivým aktivům je dáno výsledkem procesu autentizace a autorizace, přičemž systém řízení přístupu umožní přístup pouze do daných segmentů datové sítě na základě pravidel pro danou identitu koncového klienta, jedná se o řízení přístupu dle protokolu IEEE 802.1X. V případě řízení administrátorského přístupu k aktivním síťovým prvkům je administrátorovi umožněn přístup pouze do definovaných oblastí spravovaného systému, jedná se o nasazení protokolu TACACS+.*
Název opatření:	*BEZPEČNOST KONCOVÝCH KLIENTŮ (OPATŘENÍ PRO REALIZACI AKTIVNÍ OCHRANY KONCOVÝCH STANIC)*
KII/VIS/ISZS/IS/KS:	*NIS TREE, MEDIOX, LIMS, VEMA, NEFRIS, ANETE, PACS, dále kompletní síťová infrastruktura.*
Popis opatření:	*Opatření navrhuje zvýšit kybernetickou bezpečnost a doplnit systém ochrany na úrovni interní sítě a perimetru o systém proaktivní ochrany přímo na koncových stanicích. Návrhem je implementace systému Endpoint Detection and Response/Endpoint Protection Platform (sw klientů na koncové stanice a servery a centralizovaného řídícího a analytického nástroje). Společně tak systém dokáže zajistit proaktivní ochranu přímo na uživatelských počítačích, dále administrátorům umožnit centrálně spravovat bezpečnostní politiky a analyzovat případné bezpečnostní incidenty a efektivně a včas zasáhnout.* *Řešení nahradí současný systém v plném rozsahu a doplní chybějící bezpečnostní funkcionality v prostředí, a to především:* • *Detekce moderních hrozeb (malware, ransomware, phishing).* • *Monitoring podezřelých aktivit v prostředí zadavatele.* • *Proaktivní ochrana před hrozbami* • *Sandboxing technologie doplňující výše jmenované.* • *Behaviorální analýza zachycených událostí za pomoci centralizovaného nástroje* • *Možnost integrace vpn klienta kompatibilního s vpn bránou.*
Sdílení opatření se ISOUI:	*Žadatel neprovozuje ISOUI.*

ID opatření:	**8.**
Oblast opatření podle ZKB a vyhlášky o kybernetické bezpečnosti:	*Navrhované řešení centrálního řízení přístupu k síti naplňuje následující body Vyhlášky:* • *§ 19, odstavec 2, písm. a) – systém vystupuje v roli autentizační a autorizačního serveru pro jak řízení přístupu k datové síti, tak pro administrátorský přístup k aktivním síťovým prvkům.* • *§ 19, odstavec 2, písm. b) – systém umožní definovat maximální možný počet neúspěšných pokusů o přihlášení před tím, než bude koncový klient zapsán na seznam blokovaných klientů a bude mu odepřen přístup.* • *§ 19, odstavec 2, písm. c) – systém používá pro autentizaci koncových klientů protokolů, které nepřenášejí privátní hesla nebo klíč přes datovou síť (PEAP-MSCHAPv2, EAP-TLS).* • *§ 19, odstavec 2, písm. e) – Systém umožní nastavení vypršení platnosti přihlášení po uplynutí určitého časového intervalu, během které klient neprovedl reautentizaci. Systém také podporuje rozšíření RADIUS protokolu o funkcionalitu Change-of-Authorization (CoA, RFC 5176), díky které lze vynutit změnu přidělených oprávnění koncovým klientů přímo z centrální systému řízení přístupu. Tímto lze reagovat i na případné změny identity (např. zneplatnění už. certifikátu nebo zamčení už. účtu v ActiveDirectory).* • *§ 19, odstavec 2, písm. g) – systém umožňuje tvorbu pravidel pro správu přístupu jak k drátové a bezdrátové síti, tak i správu administrátorských přístupů k aktivním síťovým prvkům. Je umožněna integrace libovolného koncového autentizačního systému, který podporuje standardní protokoly RADIUS nebo TACACS+. Správa pravidel a identit je prováděna přes jednotné rozhraní systému i v případě, kdy je řešení implementuje dva či více redundantních autentizačních serverů.* *Návaznost na § 20.* • *písm. a) – řízení přístupu k jednotlivým aktivům je dáno výsledkem procesu autentizace a autorizace, přičemž systém řízení přístupu umožní přístup pouze do daných segmentů datové sítě na základě pravidel pro danou identitu koncového klienta, jedná se o řízení přístupu dle protokolu IEEE 802.1X. V případě řízení administrátorského přístupu k aktivním síťovým prvkům je administrátorovi umožněn přístup pouze do definovaných oblastí spravovaného systému, jedná se o nasazení protokolu TACACS+.*
Název opatření:	*nasazení přístupového z a zabezpečovacího systému na serverovny a jednotlivé racky*

KII/VIS/ISZS/IS/KS:	*NIS TREE, MEDIOX, LIMS, VEMA, NEFRIS, ANETE, PACS, dále kompletní síťová infrastruktura.*
Popis opatření:	*V rámci tohoto projektu je počítáno s nasazením zabezpečení serverovny jak na úrovni místnosti, tak na úrovni rackové skříně s daty. Pro zabezpečení místosti je plánován standardní PZTS systém dle normy ČSN EN 50131-1 ed. 2. Systém bude střežit samotný plášť místnosti (okna, dveře) ale také potenciální pohyb přímo v místnosti, a to pomocí PIR čidel. V případě neoprávněného vstupu dojde k aktivací vnitřní sirény, odeslání zprávy na pult centrální ochrany a také formou SMS na vybrané pracovníky. Do systému budou doplněny i environmentální senzory pro redundantní kontrolu teploty v místnosti (řešeno i v rámci rackové skříně) a také detektory kouře pro případ vzniku požáru*
Sdílení opatření se ISOUI:	*Žadatel neprovozuje ISOUI.*

4.2.3 Podrobný popis konečného stavu po realizaci projektu

Po realizaci projektu bude dosaženo zvýšení kybernetické bezpečnosti informačních Nemocnice. Tohoto cíle bude dosaženo realizací několika dílčích cílů zaměřených na řešení uvedených problémů. Dílčími opatřeními jsou:

1) Pořízení nových páteřních přepínačů
   Naplnění vyhlášky č. 82/2018 Sb, část druhá, hlava II a to:
   - 18, písm. a) – zajištění segmentace sítě pomocí VLAN tagging (IEEE 802.1Q).
   - § 18, písm. c) – zajištění důvěrnosti a integrity dat při přenosu dat přes páteřní spoje pomocí šifrovacího protokolu MACsec.
   - § 19, odstavec 2, písm. a) –autentizace přístupu k administraci páteřních přepínačů pomocí protokolu TACACS+, kdy je kontrolována identita administrátorského uživatele.
   - § 20, písm. b) – autorizace přístupu k jednotlivým částem operačního systému přepínače a jejich konfiguračních změn prostřednictvím protokolu TACACS+ a to na základě identity a role administrátorského uživatele.
2) Pořízení nových serverů a diskových polí
   Naplnění vyhlášky č. 82/2018 Sb, část druhá, hlava II a to:
   Řešení z technického pohledu naplňuje dle § 19 odstavce 1 požadavek na zajištění nástroje pro správu a ověření identity aplikací informačního a komunikačního systému. Podle odstavce 2 je nástrojem pro ověření identity aplikací a výpočetních komponent - ověří

identitu před zahájením výpočetních aktivit a zajistí centralizovanou správu identit výpočetních systému jako takových.
Technické řešení současně naplňuje dle § 27 bodu a) až d) požadavek na zajištění:

- dostupnosti informačního a komunikačního systému pro splnění cílů podle § 15,
- odolnosti informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům, které by mohly snížit jeho dostupnost,
- dostupnosti důležitých technických aktiv informačního a komunikačního systému a
- redundance aktiv nezbytných pro zajištění dostupnosti informačního a komunikačního systému.

3) Pořízení nástroje pro zajištění síťové bezpečnosti
Opatření navrhuje zvýšit jak kybernetickou bezpečnost, tak zajištění vysoké dostupnosti implementací firewall řešení v konfiguraci HA (high availability) clusteru. Jednotlivé prvky firewallu budou fyzicky umístěný již v existujících oddělených DC zadavatele a z pohledu topologie sítě bude firewall připojen k core infrastruktuře. V plném rozsahu bude nahrazen současný hardware a jeho funkcionalitu přebere nové řešení, současně bude pak doplněno o funkcionality nové, a to především:

- Segmentace interní LAN a následná možnost kontroly provozu.
- Integrace s centrálním zdrojem identit (AD) a kontrola provozu na granulární úrovni.
- Aktivní ochrana před kybernetickými hrozbami za pomocí modulů IPS, antimalware, antiransomware, AV, antibot apod.
- Sandboxing technologie doplňující výše jmenované.
- Implementace logserveru umožňující centrální sběr a analýzu logů.

Cílová situace ohledně kybernetické bezpečnosti Nemocnice by po aplikaci zmíněných opatření měla být taková, aby její zaměstnanci měli povědomí o bezpečnostních rizicích, vyvarovali se rizikového chování a dokázali pružně a efektivně reagovat na nastalé bezpečnostní incidenty. Do cílového stavu lze zahrnout i určité zajištění prevence před bezpečnostními incidenty, čehož bude dosaženo, jak výše uvedenými opatřeními, tak speciálními nástroji pro monitoring a analýzu síťového provozu. Vytvoření dokumentace a zavedení pravidel pak umožní v kombinaci se systémy pro detekci bezpečnostních incidentů včasnou reakci na tyto incidenty a jejich řešení.

4.3 Odůvodnění potřebnosti a účelnosti investice

a) Stručné zdůvodnění záměru

Potřebnost realizace předkládaného projektu vyplývá z cíle žadatele zvýšit zabezpečení vůči kybernetickým hrozbám a dále z připravované změny legislativy. Vývoj ICT neustále postupuje a tím se rozšiřuje možný okruh případných relevantních hrozeb pro ICT zařízení žadatele. Roste rovněž dostupnost ICT vybavení i rychlost případných nekalých praktik, jakož i informovanost v ICT oboru. Současně je digitalizováno maximálního množství procesů a dat nejen v přímém poskytování lékařské péče, ale i v podpůrných souvisejících činnostech nemocnice. Žadatel se proto rozhodl na základě zvážení aktuálního stavu svého ICT vybavení, průzkumu současných možností v oblasti zabezpečení, požadavků managementu společnosti a finančních možnosti využití dotace k zajištění odpovídajícího zabezpečení, jenž by zamezilo případným útokům. Na základě platné legislativy je žadatel povinen zabezpečit své informační a komunikační systémy, a to účelně a hospodárně. Studie proveditelnosti zpracovává záměr výrazného zvýšení zabezpečení a dostupnosti kritických informačních systémů Nemocnice s poliklinikou Česká Lípa. Východiskem pro zpracování studie proveditelnosti byly dva po sobě následující kybernetické útoky, kterým musela nemocnice čelit a následná havárie kritické

informační infrastruktury. Na základě zkušeností s alespoň částečnou nápravou a obnovením provozu do prozatím nouzového režimu byl tento projekt navržen tak, aby přinesl především:

- zvýšení zabezpečení komunikační sítě,
- zvýšení zabezpečení IS a zpracovávaných citlivých dat,
- zvýšení zabezpečení záloh IS,
- zásadní zvýšení dostupnosti IS,
- maximální možnou ochranu proti průniku škodlivého kódu,
- řízení privilegovaných účtů,
- zavedení nástroje prevence úniku dat.

b) Vazba projektu na specifický cíl 1.1 a výzvu

Projekt je plně v souladu s Integrovaným regionálním operačním programem 2021 - 27, Specifickým cílem 1.1 Využívání přínosů digitalizace pro občany, podniky, výzkumné organizace a veřejné orgány, jakož i s výzvou č. 3 Kybernetická bezpečnost – SC 1.1 (MRR). Místem realizace projektu je Liberecký kraj, projekt je zaměřen na realizaci technických bezpečnostních opatření podle hlavy II, vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

c) Identifikace dopadů a přínosů projektu s důrazem na popis dopadů na cílovou skupinu

Projekt umožní zajistit zabezpečení informačního systému žadatele – Nemocnice s poliklinikou Česká Lípa, který je významným poskytovatelem zdravotních služeb v regionu. Tím bude mít výrazný pozitivní dopad zejména pro obyvatele regionu, kterým projekt umožní využívat služby nemocnice bez ohledu na možné hrozby kybernetických útoků související s možností vyřazení informačního systému nemocnice, ztrátou či zneužitím dat apod.

Realizace projektu bude mít pozitivní přínos pro všechny cílové skupiny projektu:

- zaměstnancům žadatele umožní vykonávat činnosti v rámci kvalitnějšího zabezpečení dat potřebných pro každodenní činnosti v rámci pracovního procesu,
- pacientům/občanům/široké veřejnosti zajistí bezproblémový průběh krátkodobého či dlouhodobého ošetření nezbytného k zajištění jejich zdraví, vyšší ochrana osobních údajů a zdravotních dat,
- managementu společnosti žadatele, s ohledem na nežádoucí únik informací a jejich možné zneužití, zajistí bezpečnější uchovávání a přenos informací,
- další řadě orgánů a institucí nejen veřejných umožní zajištění odpovídajícího propojení s ohledem na relevantní požadavky dané oblasti;
- žadateli o dotaci - Nemocnici s poliklinikou Česká Lípa zajistí zvýšení kybernetické bezpečnost IS na úroveň, která je požadována v rámci standardů zákona č. 181/2014 Sb., o kybernetické bezpečnosti; snížení pracnosti při správě systémů a odolnosti systému proti kyberbezpečnostním hrozbám při očekávaném nárůstu počtu sofistikovaných kybernetických útoků s vyšší mírou diverzifikace, se kterými se žadatel, spravující osobní a citlivé údaje, musí vypořádat.

Dopad na cílové skupiny projektu je uveden také v Kapitole 3 Studie proveditelnosti.

d) Zdůvodnění potřebnosti pořizovaného vybavení / majetku

Identifikace pořizovaného majetku byla definována v rámci technické specifikace projektového záměru s ohledem na požadavky týkající se kvalitního zajištění a zabezpečení informačního systému žadatele. Počty pořizovaných kusů odpovídají požadavkům systému, tak aby bylo jeho zabezpečení komplexní, účinné a bezproblémové. Tyto byly identifikovány osobami projektového týmu (viz dále) ve spolupráci s externími subjekty tak, aby projekt vyhovoval parametrům dotačního titulu a výzvy. Umístění jednotlivých prvků je v souladu s pravidly logického uspořádání systému, konkrétními prostory v objektu žadatele i požadovanými nároky na obslužnost a servis daných zařízení.

e) Popis souladu projektu s Prováděcím dokumentem programu Digitální Česko pro čerpání z IROP 2021-27

Předkládaný projektový záměr je plně v souladu s Prováděcím dokumentem programu (viz výše), které vydalo Ministerstvo vnitra a podporuje Hlavní cíle IK ČR (Informační koncepce České republiky), kterými v oblasti Kybernetické bezpečnosti jsou (viz str. 12 dokumentu). Je zaměřen zejména na následující:

- Cíl č. 1 „Uživatelsky přívětivé a efektivní on-line služby pro občany a firmy“.

Částečně nepřímým efektem dojde sekundárně i k napojení na cíle:

- Cíl č. 3 „Rozvoj prostředí podporujícího digitální technologie v oblasti eGovernmentu“
- Cíl č. 5 „Efektivní a centrálně koordinované ICT veřejné správy“.

Projekt je v souladu s kapitolou 3.2.7 Kybernetická bezpečnost, neboť je zaměřen na realizaci technických bezpečnostních opatření podle § 5 odst. 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a mezinárodních standardů a norem v oblasti bezpečnosti informací. Prováděcí dokument dále definuje, že v rámci zabezpečení KII/VIS/ISZS/IS/KS, s výjimkou systémů určených k ochraně utajovaných informací, je možné realizovat následující technická opatření:

- fyzická bezpečnost,
- nástroj pro ochranu integrity komunikačních sítí,
- nástroj pro ověřování identity uživatelů,
- nástroj pro řízení přístupových oprávnění,
- nástroj pro ochranu před škodlivým kódem,
- nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů,
- nástroj pro detekci kybernetických bezpečnostních událostí,
- nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
- aplikační bezpečnost,
- kryptografické prostředky,
- nástroj pro zajišťování úrovně dostupnosti informací a
- bezpečnost průmyslových a řídicích systémů.

S ohledem na informace uvedené v předchozích částech této Studie proveditelnosti, je jasné, že uvedené projekt splňuje.

f) Zdůvodnění potřebnosti stavby, přístavby, nástavby a stavebních úprav (rekonstrukce, modernizace)
Uvedené je nerelevantní, projekt nezahrnuje stavební opatření.

g) Alternativní řešení

- Zdůvodnění, proč byla nulová varianta (ponechání stávajícího stavu) posouzena jako nevyhovující. Nulová varianta projektu představuje situaci, kdy nedojde k realizaci projektu, ale

nemocnice bude muset vynaložit prostředky na pořízení dílčích technologií na zajištění bezpečnosti, ochrany a dostupnosti IS. S ohledem na omezené investiční zdroje žadatele v této oblasti hrozí, že postupně pořizované vybavení nezajistí potřebnou a komplexní ochranu a dostupnost infrastruktury a nebudou tak eliminována bezpečnostní rizika a potenciální kybernetické útoky, které jsou v poslední době v oblasti zdravotnictví časté. V důsledku toho může být omezena kvalita poskytování zdravotní péče v regionu.
Nulová varianta by tak mohla být pro osoby z cílové skupiny v krajním případě fatální, s ohledem na předmět činnosti žadatele, kterým je poskytování lékařské péče. Jelikož velké množství dat nezbytných např. k realizaci lékařských operací, jakož i údaje o stavu nebo např. lécích pacientů jsou uchovány elektronicky, vyřazení ICT provozu případným útokem by znamenalo pozastavení některých činnosti nemocnice, což by v případě např. neodkladných operací mohlo zapříčinit v krajním případě i úmrtí některých pacientů. Při narušení integrity uchovávaných dat může dojít ke změně v systému a tím následně k rozhodování na základě chybných nebo neúplných informací.

- Popis alternativních řešení a jejich slabých a silných stránek.
  Alternativního řešení z hlediska věcného není pro projekt možné. Řešení vychází ze všeobecně známých principů kybernetické ochrany. Žádná jiná alternativa neposkytuje možnosti pojmout zabezpečení komplexně a v návaznosti na všechny oblasti kybernetické zabezpečení. Některé z alternativ by naopak v budoucnu mohly přinést další problémy a zvýšené náklady.
  Alternativní řešení z hlediska finančního by představovalo realizaci projektu pouze z vlastních zdrojů žadatele bez obdržené dotace. Tato skutečnost by znamenala výrazné prodloužení realizace projektu s ohledem na aktuální finanční možnosti žadatele a tím by mohla ohrozit zajištění včasného zabezpečení IS žadatele proti kybernetickým útokům.
- Porovnání alternativ: jak bylo uvedeno v odstavci výše, alternativy byly filtrovány při samotné tvorbě technického řešení s ohledem na maximální přínos projektu. Jiné alternativní řešení projektu není, pro žadatele je nezbytné realizovat předkládaný záměr s ohledem na zajištění bezpečnosti spravovaných dat.
- Zdůvodnění vybrané alternativy, zejména zdůvodnění hospodárnosti, účelnosti a efektivnosti vybrané alternativy: jak bylo uvedeno výše, alternativní řešení neexistuje, drobné rozdíly v pořizovaném technickém řešení byly filtrovány při jeho tvorbě.

h) Vymezení všech zainteresovaných subjektů a jejich členění
Žadatelem o dotaci, vlastníkem i provozovatelem IS je Nemocnice s poliklinikou Česká Lípa, a.s. Zakladatelem žadatele je Liberecký kraj.

4.4 Harmonogram realizace projektu

Aktivita	Předpokládaná lhůta	Termín
ZAHÁJENÍ REALIZACE PROJEKTU (podpis smlouvy na zpracování Studie proveditelnosti a přípravy žádosti o dotaci)		**11.7.2022**
Příprava projektu včetně personálního a organizačního zajištění projektu, definice technického řešení, zpracování Studie proveditelnosti, žádosti o dotaci, zajištění příloh k žádosti o dotaci	Cca 1 měsíc	Do 16.8.2022

Aktivita	Předpokládaná lhůta	Termín
Hodnocení žádosti o dotaci	110 pracovních dnů od odevzdání žádosti o dotaci + aktuální odhad	Do 30.9.2023 (při odevzdání žádosti o dotaci v 1. den výzvy
Rezerva na doplňování žádosti o dotaci (max. 2 doplnění, na jedno doplnění max. 5 pracovních dnů, možno prodloužit o dalších max. 5 prac. dnů)	10 pracovních dnů	Zahrnuta do doby v řádku výše
Realizace výběrového řízení na dodavatele včetně časové rezervy Příprava a vydání právního aktu / Rozhodnutí	Cca 4,5 měsíce	**1.10.2023 – 15.2.2024**
Fyzická realizace přímých nákladů projektu (realizace dodávek/služeb v rámci podepsané smlouvy o dílo)	9 měsíců	**16.2.2024 – 15.11.2024**
UKONČENÍ REALIZACE PROJEKTU		**15.11.2024**
Předložení žádosti o platbu a závěrečné zprávy o realizaci	20 pracovních dnů	**15.12.2024**
Udržitelnost projektu z hlediska dotace IROP	5 let	**do r. 2029**

Návaznost jednotlivých částí harmonogramu

- Harmonogram je uveden včetně předpokládaných časových rezerv.
- Jednotlivé časové období na sebe vzájemně navazují s ohledem na svoji provázanost. V případě výraznějšího prodloužení/zkrácení předchozího časového období bude následné časové období relevantně zahájeno později/dříve s ohledem na zajištění požadavků jednotlivých fází a zájem žadatele zrealizovat projekt v co nejkratším časovém rozsahu při zachování kvality jednotlivých částí.

- Realizace jednotlivých dodávek / služeb bude uskutečněna po výběru dodavatele a podpisu smlouvy o dodávce / službách.
- Datem ukončení realizace projektu se rozumí termín, kdy dojde k naplnění účelu projektu.
- Datum podepsání dokladu o předání a převzetí nesmí překročit termín ukončení realizace projektu, uvedený v PA/Rozhodnutí. Součástí dokladu o předání a převzetí díla může být seznam vad a nedodělků, které však nesmí bránit plnění účelu projektu. Pokud uvedené vady a nedodělky brání plnění účelu projektu, nelze projekt považovat za ukončený. Žadatel si je vědom skutečnosti, že dokumentace dokládající ukončení realizace projektu, která je přílohou závěrečné zprávy o realizaci, musí být vystavena s datem v době realizace projektu.
- Projekt bude realizován dle výše uvedeného harmonogramu pouze v případě schválení žádosti o dotaci, pokud žádost o dotaci schválena nebude, bude uskutečněn pravděpodobně v podstatně delším časovém úseku s ohledem na aktuální disponibilní finanční prostředky žadatele.

Sledovaná období projektu

(V programovém období EU 2014 – 20 nazýváno etapizací, ta pro nové období 2021 – 27 „nahrazena“ sledovanými obdobími.)

Pokud to bude umožněno dle pokynů k dané výzvě, bude fyzická realizace projektu (16.2.2024 – 15.11.2024) rozdělena na 2 sledovaná období, každé v délce cca 4,5 měsíce:

- 1. sledované období: 16.2.2024 – 30.6.2024, předložení žádosti o platbu do 29.7.2024 ;
- 2. sledované období: 1.7.2024 – 15.11.2024, předložení žádosti o platbu do 15.12.2024.

Žadatel si je vědom skutečnosti, že sledovaná období končí vždy 20 pracovních dnů před plánovaným předložením žádosti o platbu uvedeným na finančním plánu. Plánovaná data předložení žádosti o platbu od sebe musí být vzdálena alespoň 3 měsíce. Sledovaná období na sebe tedy musí časově navazovat a nesmí se překrývat.

4.4 Připravenost projektu k realizaci

4.4.1 Technická připravenost

- Projektová dokumentace:
  - technická specifikace obsahu projektu byla komplexně vyhotovena před podáním žádosti o dotaci, tedy v srpnu 2022,
  - projektová dokumentace stavby - není relevantní, projekt neobsahuje stavební práce.
- Výběrové řízení na přípravu žádosti o dotaci proběhlo v červenci až srpnu 2022, dne 11.7.2022 byla uzavřena smlouva s dodavatelem, který je i zpracovatelem předkládané studie proveditelnosti – identifikační údaje viz kapitola 1 této studie.
- Výběrové řízení na dodavatele hlavního předmětu projektu se předpokládá, že bude realizováno v termínu březen až červen 2023, dle harmonogramu v podkapitole výše v rámci následujícího vymezení:
  - předpokládaný typ kontraktu zadávacího řízení: smlouva,
  - předpokládaný předmět veřejné zakázky: dodávky a služby,
  - specifikace druhu zadavatele: veřejný,
  - veřejná zakázka dle výše předpokládané hodnoty: nadlimitní.
  - druh zadávacího řízení: otevřené řízení.
- Stav závazných stanovisek dotčených orgánů státní správy: k datu podání žádosti o dotaci bylo zažádáno o stanovisko odboru Hlavního architekta eGovernmentu, viz přílohy k žádosti o dotaci v rámci ISKP 2021+. Jakmile žadatel stanovisko obdrží, bude doloženo do příloh v rámci ISKP 2021+.
- Doklady prokazující povolení umístění stavby a dokladů prokazujících povolení k realizaci stavby dle zákona č. 183/2006 Sb., o územním plánování a stavebním řádu (stavební zákon), ve znění pozdějších předpisů: není relevantní – předmětem realizace předkládaného projektu nejsou stavební práce.

4.4.2 Finanční připravenost

Dotace / vyrovnávací platba je uvažována vzhledem k pravidlům výzvy ve výši 85%. Místo realizace projektu je Liberecký kraj, Žadatel o dotaci je organizace založená krajem.

Předfinancování a kofinancování projektu bude uskutečněno jak s využitím vlastních zdrojů žadatele, v případě potřeby tak s ohledem na výši projektu i s využitím bankovního úvěru žadatele (to se týká pravděpodobně zajištění předfinancování projektu, které bude následně kryto dotací). Nemocnice s poliklinikou Česká Lípa, a.s. dlouhodobě spolupracuje s bankovní institucí při kofinancování projektů

realizovaných nejen s využitím dotačních zdrojů EU. Předfinancování a kofinancování se uvažuje dle harmonogramu realizace projektu s přihlédnutím k možnému rozdělení projektu na jednotlivá časová období, viz informace ve formuláři žádosti o dotaci.

4.4.3 Administrativní připravenost

Projektový tým je složen z osob uvedených v následující tabulce. Členové projektového týmu se nemění po celou dobu realizace projektu od přípravy projektu až po zajištění udržitelnosti. Všichni členové projektového týmu jsou dlouhodobí zaměstnanci Nemocnice s poliklinikou Česká Lípa, a.s.

Pozice v projektu	Jméno a příjmení	Pracovní pozice	Vzdělání, praxe, zkušenosti s projekty	Odpovědnosti a pravomoci v přípravné/realizační i provozní fázi projektu
Manažer projektu	Vladimír Matoušek	Vedoucí oddělení ICT	23 let praxe v IT, SŠ vzdělání	Management projektu, specifikace projektu z hlediska obsahového
Zástupce manažera projektu	Ing. Roman Viceník	ICT specialista Architekt kybernetické bezpečnosti	25 let praxe, VŠ vzdělání	Zastoupení manažera projektu, koordinace projektu ve vztahu k externím subjektům, specifikace projektu z hlediska technického
Personální specialista	Mgr. Pavlína Pilařová	Personální ředitelka	13 let praxe, VŠ vzdělání	Koordinace v rámci požadavků/dopadu projektu na zaměstnance nemocnice
Specialista kvality	Ing. Alena Brodská	Manažerka kvality	11 let praxe, VŠ vzdělání	Koordinace v rámci požadavků na zajištění kvality poskytovaných služeb nemocnicí
Vedoucí ekonom projektu	Ing. Petr Urban	Ekonomický ředitel	17 let praxe, VŠ vzdělání	Koordinace projektu z hlediska zajištění finančních zdrojů/finančních toků
Ekonomka projektu	Miluše Prokopová	Hlavní účetní, ekonomický odbor	25 let praxe, SŠ vzdělání	Zajištění ekonomických podkladů/účetní stránky projektu

Všichni členi projektového týmu mají znalosti a zkušenosti odpovídající jejich začlenění na jednotlivé pozice v týmu, které navazují na jejich pracovní pozice a mají zkušenosti s realizací projektů včetně dotací EU. Je zajištěna 100% zastupitelnost všech osob týmu, jejich pravomoci a zodpovědnosti jsou v rovnováze.

Popis organizačních a finančních vztahů mezi příjemcem podpory a provozovatelem v době realizace:
není relevantní – žadatel o dotaci je rovněž provozovatelem.

4.6. Ekonomická / neekonomická činnost žadatele o podporu

Účelem a předmětem činnosti organizace žadatele jsou dle výpisu z rejstříku následující činnosti:

- poskytování lůžkové, ambulantní a další zdravotní péče v rozsahu registrace podle zákona č. 160/1992 Sb., o poskytování zdravotní péče v nestátních zdravotnických zařízeních, v platném znění,
- poskytování knihovnických a informačních služeb,
- hostinská činnost,
- masérské, rekondiční a regenerační služby,
- výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona,
- zámečnictví, nástrojářství,
- vodoinstalatérství, topenářství.

Ekonomickou činností se v souladu s rozhodovací praxí Evropské komise rozumí nabízení zboží a/nebo služeb na trhu. Všechny výše specifikované služby lze tedy považovat za ekonomické, i přestože jsou některé provozovány v minimálním rozsahu. To se týká zejména knihovnických služeb (je zde některým uživatelům účtován malý poplatek).

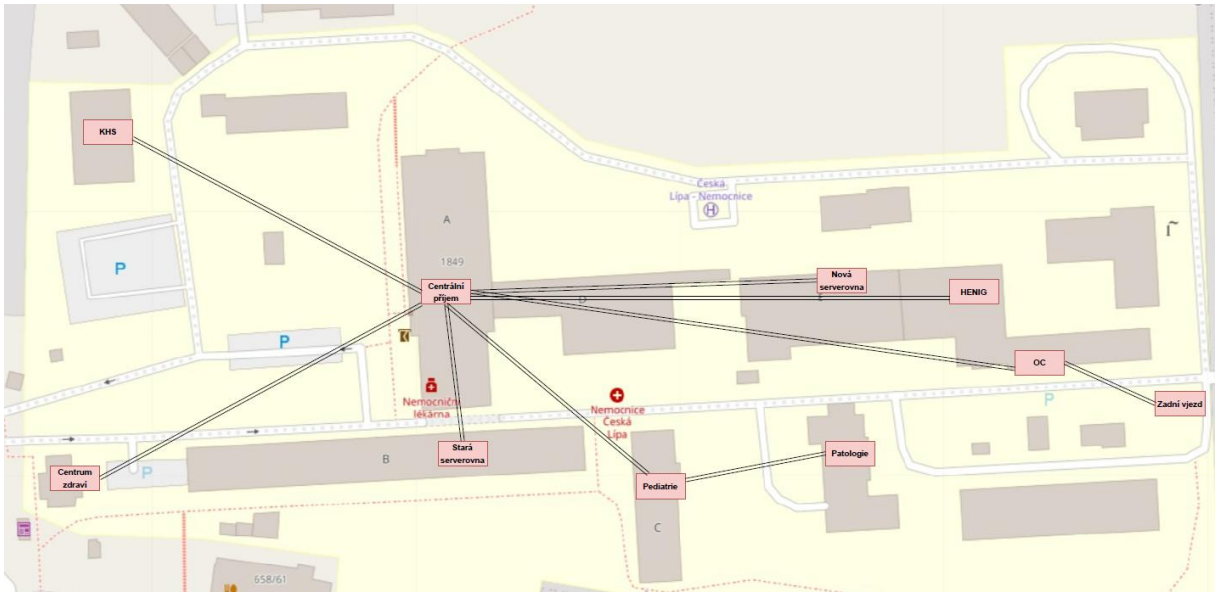
Nicméně, žadatel o dotaci – Nemocnice s poliklinikou Česká Lípa, a.s. vykonává služby obecného hospodářského zájmu, k čemuž jí byl vydán Pověřovací akt v souladu s rozhodnutím Komise. Podrobně viz kapitola Veřejná podpora.

Žadatel nevede oddělené účetnictví pro činnosti ekonomické a činnosti neekonomické.

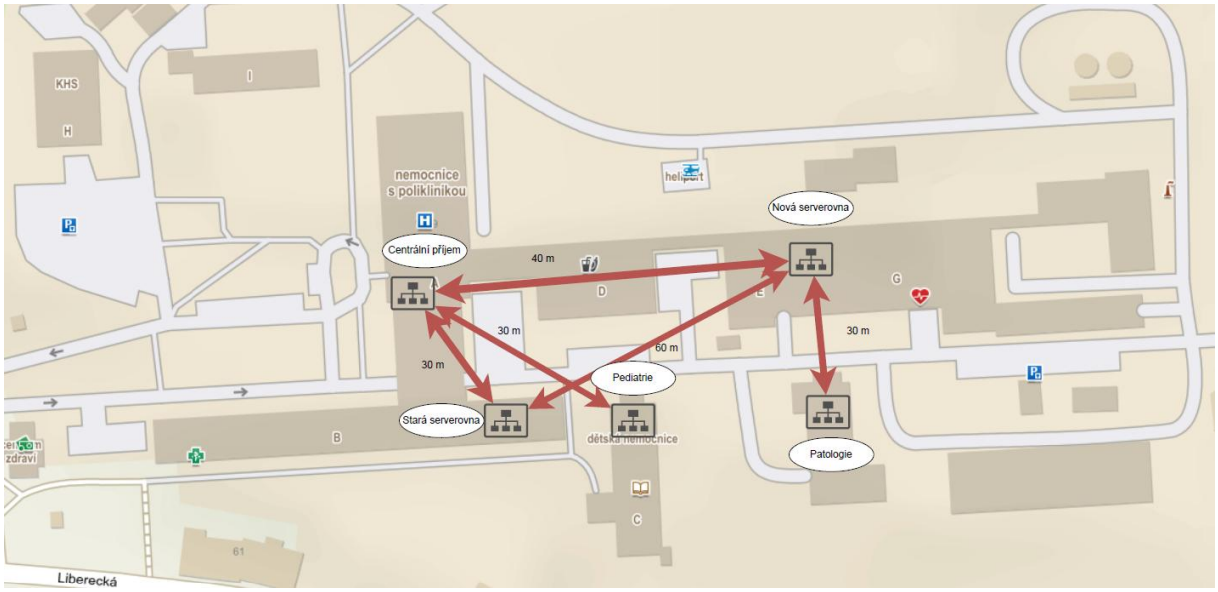
5. PROKÁZÁNÍ PRÁVNÍCH VZTAHŮ

Místo realizace předkládaného projektu je zobrazeno na následujících mapách areálu Nemocnice s poliklinikou Česká Lípa, a.s.

Obrázek níže uvádí aktuální zasíťování.



Následující vyobrazení představuje optiku páteřní sítě.



Všechny stavby/pozemky/movité věci jsou ve vlastnictví žadatele o dotaci – Nemocnice s poliklinikou Česká Lípa, a.s. Pozemky / stavby nejsou zatíženy cizími právy ve smyslu zástav nemovitostí / věcných břemen / úvěrů apod. (jsou zde pouze práva vztahující se k umístění sítí z hlediska územního).

Místa realizace prostor, které se nejvíce vztahují k předmětu projektu, jsou uvedena v tabulce níže (dle optiky páteřní sítě). Kompletní výčet vztažený k pozemkům a stavbám nemocnice je pak přiložen ve výpisu z katastru nemovitostí v přílohách na záložce Dokumenty k žádosti o dotaci.

Nemovitá věc v katastrálním území 621 382 Česká Lípa	
Parcelní číslo	**Právní vztah**
728/42 stará serverovna	Vlastnictví žadatele
728/23 – nová serverovna	
p. č. 728/3 centrální příjem	
p. č.728/35 pediatrie	
728/50 Patologie	

Movitý majetek

Movitá věc (uvést výčet)	**Právní vztah**
Podrobný výčet nejdůležitějších movitých statků je uveden v ISKP 2021+ v Dokumentech jako samostatná příloha: NemCL_seznamy_stavajici_vybaveni_zarizeni_IS	Vlastnictví žadatele

6. SOULAD PROJEKTU S PRINCIPY ZAJIŠŤUJÍCÍMI ROVNOST, ZAČLENĚNÍ A NEDISKRIMINACI A S PRINCIPY UDRŽITELNÉHO ROZVOJE (HORIZONTÁLNÍ PRINCIPY)

6.1 Soulad projektu s principy zajišťujícími rovnost, začlenění a nediskriminaci

Projekt má neutrální dopad na genderovou rovnost a nediskriminaci.
Projekt není přímo zaměřen na řešení rovných příležitostí a nediskriminaci, proto je jeho vliv do této oblasti obecně neutrální. Přesto má lehce pozitivní dopad na rovné příležitosti, neboť zajišťuje mimo jiné bezpečnost dat všech, bez rozdílu genderu s ohledem na nediskriminaci jakýchkoliv skupin osob. Rovněž při přípravě a realizaci projektu, jakož i ve fázi provozu nejen po dobu udržitelnosti, bude dbáno na zachování rovného přístupu a nediskriminace. To se týká také zejména zajištění přístupových práv do systému, zadávání vstupních dat a získávání výstupů z jednotlivých části IT systému nemocnice. Zajištění rovného přístupu a nediskriminace je rovněž řešeno v rámci interních dokumentů nemocnice, týkající se jak zaměstnanců, tak i pacientů. A to v rovině personální i v oblasti poskytování konečné služby tedy zdravotní péče jednotlivým pacientům. Dále je dbáno na zajištění přístupu i pro osoby se zdravotním postižením v souladu s národními a mezinárodními standardy. Obecně lze konstatovat, že projekt nebude svým zaměřením mít žádný negativní vliv na rovnost, začlenění a nediskriminaci osob.

6.2 Soulad projektu s principy udržitelného rozvoje

Projekt má neutrální dopad na udržitelný rozvoj.
Projekt není přímo zaměřen na řešení principů udržitelného rozvoje. Přesto má částečně pozitivní dopad do oblasti životního prostředí. Jednotlivé IT systémy v rámci projektu nahrazují původně využívané papírově tištěné metody uchování dat a komunikace. Zajištění a zabezpečení elektronického prostředí dat tak pozitivně dopadá na jednotlivé body uvedené níže, týkající se např. omezení využívání tištěné dokumentace v rámci jednotlivých procesů, vhodnějšího organizačního uspořádání jednotlivých procesů v rámci nemocnice zajišťující kvalitnější logistiku osob/služeb/materiálu atd., kvalitnější logistiku v rámci zajištění. Rovněž kvalitnější zabezpečení celého IT systému zajišťuje vyšší důvěryhodnost elektronických dat a tím zmenšuje počet potřebných tištěných materiálů pro potřeby denní komunikace, ale i např. archivace apod. Nový IT systém zabezpečuje také řízení energetických zdrojů nemocnice apod., jsou zde umístěny měřiče spotřeb, jenž umožní snížení požadovaných energetických vstupů do systému.
Neutrální či pozitivní dopad na udržitelný rozvoj je řešen rovněž v rámci každodenního chodu jednotlivých oddělení nemocnice, zejména co se týká logistiky, zajištění materiálu či nakládání s odpady.

<u>Vlivy projektu na klima a vlivy klimatu na výstupy projektu</u>
Realizací projektu nedojde ke zvýšení emisí skleníkových plynů a bude zajištěna klimatická odolnost infrastruktury; nižší využití tištěné dokumentace umožňuje omezení dopadu na klima, snížení spotřeby papíru, zachování lesů a tím omezení klimatických změn, apod., viz výše. Vzhledem ke skutečnosti, že ICT nemocnice řeší také energetické úspory, bude mít ve svém důsledku nižšího využití vstupních energií dopad na snížení emise skleníkových plynů. Rovněž zajištěním ICT bezpečnosti dojde ke zkvalitnění logistiky v rámci nemocnice a tím i např. tvorbě nižších zásob, což má za příčinu nižší klimatickou stopu.

Vlivy na udržitelné využívání a ochranu vodních zdrojů

Realizací projektu nedojde k negativnímu ovlivnění povrchových a podzemních vod. Opět vyšším využitím IT dat a tím nižšímu použití tištěných médií dojde k omezení spotřeby vstupů v podobě dřeva, což má pozitivní dopad také na těžbu a tím povrchové a podzemní vody, jakož i úspory vody v procesu výroby papíru.

Opatření týkající se předcházení vzniku odpadů a recyklace

Předmětem realizace předkládaného projektu nejsou stavební práce. Nicméně v rámci pořízení nového ICT vybavení bude dbáno na řádné třídění odpadu umožňující recyklaci. Rovněž ušetřením původní tištěné formy dat oproti stávajícím datovým informacím v elektronickém prostředí dojde k výraznému předcházení vzniku odpadů. Zajištění bezproblémové funkčnosti celého systému jen podpoří jeho důvěryhodnost a spolehlivost, čímž opět podporuje využívání elektronického prostředí před vytištěným textem.

Opatření týkající se prevence a omezování znečištění ovzduší, vody nebo krajiny

Realizací předkládaného projektu nedojde ke zvýšení emisí znečišťujících látek.
Sekundárně využívání IT dat umožňuje zajistit, jak bylo uvedeno výše, např. lepší logistiku v rámci nemocnice a tím opět omezit např. množství výjezdů vozidel, zkvalitnění koordinace tepelných i elektrických zdrojů apod. Vše uvedené má pozitivní dopad na ovzduší, vodu a tím i krajinu.

Opatření na ochranu a obnovu biologické rozmanitosti a ekosystémů

Realizací předkládaného projektu nedojde k negativnímu ovlivnění zvláště chráněných území, soustavy Natura 2000 a zvláště chráněných druhů rostlin a živočichů. Místo realizace projektu se nachází mimo tyto lokality.
Jak uvedeno výše, projekt má obrácený aspekt, kdy omezení negativního dopadu na životní prostředí vlivem využívání IT dat umožní ve výsledku zachovat biologickou rozmanitost a různorodé ekosystémy.

7. VÝSTUPY A VÝSLEDKY PROJEKTU

Přehled výstupů projektu a jejich kvantifikaci

- Počet kyberneticky zabezpečených systémů nemocnice: 7.
- Počet technických opatření podpořených v rámci projektu: 8.
- Počet písmen dle § 5, odst. 3, zákona č. 181/2014 Sb naplněná projektem: 11 (g,e,i,a,f,b,d,h,c. j, k).

Uvedené výstupy naplňují cíle projektu specifikované v počátečních kapitolách této studie proveditelnosti i cíle výzvy v rámci dotačního titulu IROP, kterými je je zajištění technických bezpečnostních opatření dle § 5, odst. 3, zákona č. 181/2014 Sb., o kybernetické bezpečnosti v rámci zajištění systému IS Nemocnice s poliklinikou Česká Lípa, a.s. a to od data ukončení realizace projektu.

Indikátory výstupu

Název a kód indikátoru	Cílová hodnota	Popis stanovení cílové hodnoty
304 002 Nové nebo modernizované prvky k zajištění standardů kybernetické bezpečnosti	7 x 11 = 77	Měrná jednotka: prvky. K naplnění cílové hodnoty indikátoru musí dojít nejpozději k datu ukončení realizace projektu. Výchozí hodnota = 0. Cílová hodnota = počet realizovaných prvků = „Počet informačních systémů žadatele, na kterých bude kybernetická bezpečnost zajištěna“ krát „počet písmen dle § 5, odst. 3, zákona č. 181/2014 Sb “. Cílová hodnota bude dosažena nejpozději k datu ukončení realizace projektu, viz kapitola Harmonogram projektu.

Žadatel si je vědom skutečnosti, že nenaplnění vykazovaného indikátoru k datu uvedenému ve Stanovení výdajů či Rozhodnutí může vést ke krácení nebo nevyplacení dotace. Jeho neudržení po dobu udržitelnosti může mít charakter porušení rozpočtové kázně s následkem finanční sankce. Sankce jsou stanoveny v Krácení peněžních prostředků při porušení Podmínek Stanovení výdajů / Rozhodnutí o poskytnutí dotace.

Významné multiplikační efekty projektu

Jednotlivé výstupy přispívají k plnění cílů projektu. Projekt bude sloužit jako další rozvoj a modernizace IS žadatele i jako nástroj pro naplnění požadavků legislativy. Zajištění ochrany IS umožní úsporu disponibilních kapacit pracovníků a umožní jim věnovat více času na řešení potřeb pacientů, případně chodu nemocnice jako takové. Díky zkvalitnění zdravotnických služeb poskytovaných pacientům tak dojde zejména ke zvýšení kvality života občanů. Dále lze předpokládat, že realizace projektu sekundárně vytvoří poptávku na vznik nových pracovních míst, a to zejména u dodavatelů řešení projektu.

Projektem nedojde k vytvoření nových pracovních míst.

Realizace předkládaného projektu však přispěje ke zvýšení důvěryhodnosti informačního systému nemocnice a tím i nemocnice jako celku, což se projeví v přístupu občanů k poskytovaným službám nemocnice a rovněž bude mít pozitivní efekt na zaměstnance subjektu žadatele v rámci jejich bezpečnější každodenní činnosti v rámci informačního systému.

8. ZPŮSOB STANOVENÍ CEN

Ceny do rozpočtu projektu byly stanoveny za účelem zjištění předpokládané výše přímých výdajů projektu.

Výběrové řízení projektu nebylo doposud zahájeno, a proto mechanismus stanovení předpokládané ceny odpovídá výběru nejnižší ceny ze tří poskytnutých nabídek možnými potencionálními dodavateli v rámci průzkumu trhu. Předmětem projektu nejsou stavební práce, tj. ani rozpočet stavebních prací.

V rámci stanovení ceny i následného výběrového řízení budou dodrženy podmínky týkající se pravidla 3E, tedy zachování zásady hospodárnosti, efektivnosti a účelnosti vynaložených prostředků ve smyslu § 2 zákona 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů. Žadatel rozumí, že Pravidlo 3E v kontextu tedy znamená co nejhospodárnější nakládání s finančními prostředky při dosažení co nejlepších výsledků vedoucích k plnění stanovených cílů.

Stanovení cen do rozpočtu projektu

Předpokládaná cena rozpočtu byla stanovena předběžným průzkumem trhu, kdy byly žadatelem osloveni 3 potencionální dodavatelé, jejichž nabídky jsou uvedeny v tabulce níže. K předběžnému průzkumu trhu došlo před podáním žádosti o dotaci v srpnu 2022, tj. ceny odpovídají aktuálním cenám na trhu.

Tabulka A Stanovení cen do rozpočtu projektu

Číslo podkladu	Podklad ze dne	Zdroj informací [1)]	Cena bez DPH	Použitá cena do rozpočtu	Princip stanovení ceny [2)]	Číslo VZ / hash VZ č. [3)]	Plánované datum zahájení VZ
1	11.8.2022	IXPERTA – Petr Jirutka	38 261 047,95	38 261 047,95 Jedná se o cenu bez DPH	Průzkum trhu, nejnižší cena	x	1.10.2023
2	12.8.2022	TELMO - Roman Rieder	40 325 834,25				
3	11.8.2022	TECHDATA – Martin Bláha	43 856 842,85				

1) *Název dodavatele, adresa ceníku, jméno experta*
2) *Průzkum trhu, zakázky se stejným či obdobným plněním, jiný způsob*
3) *Pokud je relevantní.*

Komentář ke stanovení ceny do rozpočtu projektu (pokud je relevantní.

Podrobné položkové rozpočty společnosti IXPERTA vstupující do přímých nákladů projektu jsou uvedeny v ISKP na záložce Dokumenty v příloze č. 25 Výčet pořizovaného vybavení.

Nemocnice s poliklinikou Česká Lípa, a.s., si je vědoma skutečnosti, že žadatel k žádosti o dotaci nedokládá všechny podklady z předběžného průzkumu trhu (komunikace s oslovenými dodavateli, předběžné nabídky). Podklady však má k dispozici a na vyžádání je doloží.

Dokladování v době realizace projektu

Žadatel si je vědom skutečnosti, že příjemce dotace je povinen v průběhu realizace jednoznačně oddělovat všechny příjmy a úplně vykazované výdaje související s projektem od ostatních příjmů a výdajů realizovaných příjemcem, mezi které se počítají i výdaje pod paušální sazbou. K oddělení příjmů a výdajů (z pohledu účetnictví „výnosů a nákladů“) bude využit jedinečný znak (např. středisko, organizace, analytický účet, číslo projektu).

9. ZAJIŠTĚNÍ UDRŽITELNOSTI PROJEKTU

Nemocnice s poliklinikou Česká Lípa, a.s. rozumí skutečnosti, že doba udržitelnosti projektu z hlediska dotace, tedy doba, po kterou příjemce musí zachovat účel, cíle a výstupy projektu, byla stanovena na pět let od provedení poslední platby příjemci ze strany ŘO IROP, tzn. od data nastavení centrálního stavu „Projekt finančně ukončen ze strany ŘO“ v MS2021+.

Žadatel zajistí, aby po celou dobu udržitelnosti v souvislostí s dotaci zajistil povinnost:

- udržet indikátory a zachovat výsledky projektu, tzn. prvky zabezpečení,
- zajistit, aby pořízené prvky kybernetické bezpečnosti sloužily svému účelu, zejména se zohledněním maximálně přípustné doby odstávky systému či akceptovatelného výpadku,
- zajistit financování veškerých výdajů spojených s provozem a údržbou pořízených prvků kybernetické bezpečnosti.
- Mít po celou dobu udržitelnosti mít zavedena organizační opatření definovaná § 5 odst. 2 zákona o kybernetické bezpečnosti.
- Uvádět ve zprávě o udržitelnosti rozsah a popis zavedených organizačních opatření včetně jejich podložení dokumenty dokladujícími jejich plnění a zajištění personálních kapacit, jako např. přehled směrnic pro používání a správu výpočetní techniky v organizaci včetně smluv o zajištění organizačních opatřeních, případně doložení pracovní náplně odpovědné osoby.

9.1 Provozní udržitelnost

Realizace projektu je nezbytná pro zajištění udržitelnosti chodu nemocnice s ohledem na citlivá data, jejichž zajištění je předmětem řešení projektu. Projektem pořízený majetek bude sloužit k zajištění kybernetické bezpečnosti nemocnice, tedy bude každodenně využíván.
Nakládání s tímto majetkem se bude řídit interními postupy, předpisy a směrnicemi žadatele tak, aby bylo znemožněno využití majetku nežádoucími osobami (včetně třetích osob a partnerů). Tyto pravidla budou implementovány v závěrečné fázi projektu a připravovány projektovým týmem ve spolupráci s dodavatelem v průběhu dodávky tak, aby k datu ukončení projektu dle harmonogramu byl systém připraven k bezproblémovému užívání.
Údržba pořízeného IT systému bude probíhat v pravidelných časových intervalech s ohledem na zachování chodu celého systému. Časový plán údržby/oprav bude dopředu stanoven, v případě potřeby např. větších aktualizací budou uživatelé informování v dostatečném předstihu. Konkrétní částky jsou uvedeny v kapitole Finanční plán této studie.

9.2 Finanční udržitelnost

Nutná obnova majetku bude zajištěna v časovém horizontu dle odstavce výše. Předpokládá se, že údržba a oprava bude uskutečňována s využitím zejména interních zaměstnanců organizace žadatele a tudíž do běžných oprav budou vstupovat zejména náklady na tyto lidské zdroje plus materiál nezbytný k zajištěný chodu projektem pořizovaného systému. Tyto i následné investice budou hrazeny prioritně z vlastních zdrojů žadatele, v případě vyšších nákladů pak pokud to bude nezbytné s využitím bankovního úvěru. Provozní i investiční výdaje v rámci nemocnice žadatele jsou dopředu plánovány a konzultovány jak s ekonomickým oddělením nemocnice, tak i managementem, a to v případě zejména větších investic. Tomuto odpovídají i měsíční či roční výhledy týkající se čerpání finančních zdrojů nemocnice.

Majetek pořízený v rámci dotace bude žadatelem pojištěn. Žadatele si je vědom doporučení příjemcům podpory v rámci IROP sjednat si pojištění majetku pořízeného z dotace IROP. Rozumí tomu, že pojištění je vhodné zejména pro případ, kdy v průběhu realizace projektu nebo v období udržitelnosti dojde ke zničení nebo poškození majetku pořízeného z dotace. Příjemce by v tomto případě nemusel být schopen naplnit účel projektu a zachovat po stanovené období výsledky realizace projektu a byl by povinen vyplacenou dotaci vrátit. Žadatel si je dále vědom skutečnosti, že pojištění majetku není povinné a výdaje na něj nejsou způsobilé.

9.3 Administrativní udržitelnost

Zajištění každodenního chodu projektu v době udržitelnosti bude mít na starosti dva zaměstnanci ICT oddělení nemocnice ve spolupráci s celým projektovým týmem, jehož jsou součástí a jenž je představen v tabulce v kapitole 4.4.3 této studie. V případě potřeby budou kontaktovány také další osoby. Jedná se tedy každodenně o 2 osoby v rámci ICT oddělení nemocnice a dále dle potřeby projektový tým ve složení 8 osob. Projekt bude v době udržitelnosti řízen manažerem projektu a zástupcem manažera projektu, kteří jej mají na starosti již od začátku projektu a mají dlouhodobé znalosti i zkušenosti v oblasti IT. Organizační opatření v souvislosti s projektem se budou dotýkat téměř všech zaměstnanců nemocnice a z toho důvodu je v projektovém týmu také personální ředitelka společnosti žadatele, se kterou budou konzultovány a nastaveny všechny relevantní pravidla týkající se zaměstnanců. Z hlediska kvality pak bude zapojena specialista kvality, za účelem implementace pravidel včetně požadovaných nároků daných zákony/směrnicemi/předpisy externími i interními. Zaměstnanci ekonomického oddělení jsou rovněž součástí projektového týmu s ohledem na zajištění finančních potřeb ve spojitosti zejména s provozem i relevantními reinvesticemi.

10. VEŘEJNÁ PODPORA

Poskytování veřejné služby v oblasti zdravotní péče

Žadatel o dotaci Nemocnice s poliklinikou Česká Lípa, a.s. poskytuje veřejnou službu v oblasti zdravotní péče podle zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů. Pověřovací akt je doložen v příloze k žádosti o dotaci v rámci ISKP 2021+.

Žadatel si je vědom skutečnosti, že poskytovatel služeb obecného hospodářského zájmu (SOHZ) musí být pověřen k výkonu SOHZ v souladu s rozhodnutím 2012/21/EU po celou dobu životnosti investice, pokud uvedený akt dobu nepokryje, budou žadatelem doloženy dokumenty dokládající jeho prodloužení, aby nebyla krácena poskytnutá dotace / vyrovnávací platba. Žadatel si je vědom skutečnosti, že do výpočtu vyrovnávací platby za výkon SOHZ nelze zahrnout odpisy investice pořízené z IROP.

11. FINANČNÍ ANALÝZA

Finanční analýza byla sestavena rozdílovou metodou, standardně používanou v rámci dotačních investičních projektů IROP. Referenční období bylo stanoveno na 10 let. Počátečním datem referenčního období je datum zahájení projektu.

Částečný odpočet DPH

Žadatel o dotaci je plátce DPH a v rámci aktivit projektu má nárok na částečný odpočet DPH, kdy je DPH kráceno pro rok 2022 ve výši 10%. Pro rok 2023 i 2024 se uvažuje i s ohledem na předcházející roky se stejnou výší krácení ve výši 10%.
Výše DPH pro aktivity projektu je tedy stanoveno následovně:

- způsobilé DPH: 21% * 0,9 = 18,9%
- nezpůsobilé DPH: 21% * 0,1 = 2,1%.

Plán cash-flow v realizační fázi projektu v členění po letech

Tabulka s náklady projektu je uvedena následovně.
Celkové způsobilé přímé náklady projektu činí 45 492 386,01 Kč a představují náklady na hlavní část projektu bez DPH včetně způsobilého DPH 18,9%. Jedná se o náklady na realizaci jednotlivých technických opatření k zajištění kybernetické bezpečnosti, na které bude uskutečněno výběrové řízení, s vítězným dodavatelem pak bude podepsána smlouva, ve které budou tyto upřesněny dle jeho nabídky.
Způsobilé nepřímé náklady projektu jsou vypočteny dle pokynů dotačního titulu ve výši 7% ze způsobilých přímých nákladů projektu. Jedná se zejména o náklady na zajištění přípravy žádosti o dotaci včetně Studie proveditelnosti, náklady na zajištění výběrového řízení, mzdy zaměstnanců podílejících se na projektu apod. dle pravidel dotační výzvy. Vzhledem ke skutečnosti, že nepřímé náklady obsahují i mzdy osob žadatele zaměstnaných na projektu, na které se nevztahuje DPH, bude skutečný poměr mezi částkou bez DPH a DPH u nepřímých nákladů stanoven až na základě skutečného čerpání těchto výdajů.
Nezpůsobilé náklady projektu představují nezpůsobilé DPH ve výši 2,1%.

NÁKLADY PROJEKTU	cena bez DPH	DPH 21% *odpočet	Celkem
Způsobilé přímé náklady projektu	38 261 047,95	7 231 338,06	**45 492 386,01**
Způsobilé nepřímé náklady projektu (7% z přímých nákladů)	2 678 273,36	506 193,66	***3 184 467,02***
Způsobilé náklady projektu celkem	40 939 321,31	7 737 531,73	***48 676 853,03***
Nezpůsobilé náklady projektu		**859 725,75**	859 725,75
Celkové náklady projektu	40 939 321,31	8 597 257,47	49 536 578,78

Způsobilé přímé náklady projektu bez DPH ve výši 38 261 047,95 Kč odpovídají předběžnému průzkumu trhu, v rámci kterého byly stanoveny ceny do rozpočtu na základě podrobných položkových rozpočtů od společnosti IXPERTA – viz kapitola 8 této Studie proveditelnosti.

Podrobné položkové rozpočty na přímé náklady

Předběžný průzkum trhu IXPERTA: soubor:	cena bez DPH	DPH 21% * 0,9 (odpočet 10% DPH)	částka včetně DPH
kalkulace fyzická bezpečnost	3 258 611,00	615 877,48	3 874 488,48
kalkulace bezpečnost	6 490 962,99	1 226 792,01	7 717 755,00
kalkulace datova centra	20 177 902,64	3 813 623,60	23 991 526,24
kalkulace networking	8 333 571,32	1 575 044,98	9 908 616,30
Celkem přímé náklady	**38 261 047,95**	7 231 338,06	45 492 386,01

Jednotlivé soubory podrobných položkových rozpočtů (kalkulace) jsou uvedeny v příloze č. 25 Výčet pořizovaného vybavení v ISKP na záložce Dokumenty.

Zdroje financování v za projekt jsou zobrazeny v následující tabulce. Žadatel uvažuje s kofinancováním projektu z vlastních zdrojů, v případě potřeby, zejména k zajištění předfinancování nákladů bude využito bankovního úvěru.

ZDROJE FINANCOVÁNÍ	
Dotace IROP 85% ze způsobilých výdajů (vyrovnávací platba)	41 375 325,08
Zdroje žadatele celkem	8 161 253,70
Vlastní zdroje žadatele - 15% ze způsobilých výdajů	*7 301 527,96*
Nezpůsobilé výdaje	*859 725,75*
Celkem	**49 536 578,78**

Financování v čase v jednotlivých letech realizace je uvedeno následovně. V prvním roce 2022 jsou uvedeny náklady spojené zejména s definováním projektu a přípravou žádosti o dotaci, v roce 2023 bude probíhat hodnocení projektu a započato výběrové řízení na dodavatele, další náklady projektu tak vzniknou až v roce 2023, kdy bude ukončeno výběrové řízení a zejména realizovaná fyzická realizace přímých nákladů projektu.

	2022	2024	2025	Kumulativní souhrn
Způsobilé výdaje	600 000,00	48 076 853,03		48 676 853,03
_Přímé náklady projektu		45 492 386,01		45 492 386,01
_Neřímé náklady projektu	*600 000,00*	2 584 467,02		3 184 467,02
Nezpůsobilé výdaje	10 597,14	849 128,61		859 725,75
Výdaje projektu celkem	**610 597,14**	48 925 981,64		**49 536 578,78**
Dotace IROP 85%			41 375 325,08	
Vlastní zdroje žadatele	610 597,14	48 925 981,64	-41 375 325,08	8 161 253,70

Plán cash-flow v provozní fázi projektu v členění po letech

V provozní fázi nebudou vznikat žádné výnosy z projektu. Provozní náklady představují maintenance a technickou podporu celého řešení projektu (HW a SW). Náklady provozní fáze budou hrazeny z rozpočtu příjemce a jsou kalkulovány na dobu udržitelnosti projektu, tzn. v délce pěti let.
Níže je uveden plán cash-flow v provozní fázi projektu v členění po kalendářních letech. Provozní výdaje byly stanoveny průměrnou cenou z průzkumu trhu (bez DPH či zohlednění inflace) a dle dlouholetých zkušeností žadatele.

	1	2	3	4	5	6	7	8	9	10
	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031
Provozní výdaje projektu * (včetně výdajů na údržbu a reinvestice)			150 000	1 500 000	1 500 000	1 500 000	1 500 000	1 500 000	1 500 000	1 500 000
Příjmy plynoucí z provozu projektu	0	0	0	0	0	0	0	0	0	0

*Jedná se o provozní výdaje, které budou hrazeny z vlastních zdrojů žadatele.

Vyhodnocení plánu cash-flow:

Protože samotný projekt negeneruje příjmy, byl kladen velký důraz na zabezpečení finančních zdrojů nejen v investiční fázi, ale především v provozní fázi projektu. Dostatek likvidních prostředků po celou dobu realizace a udržitelnosti projektu je zaručen zajištěním dlouhodobého zdroje krytí záporných cash flow z rozpočtu příjemce a z dotace. Likvidita je dále podpořena uváženým navržením harmonogramu s dostatečným prostorem na realizaci aktivit projektu. Projekt je již ze samotného začátku koncipován jako finančně udržitelný.

Vzhledem k negativnímu cash-flow v průběhu celé realizace i provozu projektu bude investiční část projektu předfinancována z rozpočtu žadatele (v případě potřeby s využitím bankovního úvěru) a dále částečně proplacena z dotace v rámci IROP v rozsahu 85 % uznatelných nákladů (výsledný příspěvek na realizační část ze strany příjemce bude ve výši 15 % uznatelných nákladů). Nezpůsobilé výdaje budu hrazeny z vlastních zdrojů žadatele. Provozní fáze bude pak plně hrazena z rozpočtu příjemce.

V přehledu finančního cash-flow je zohledněn předpoklad průběžného proplácení vynaložených investičních nákladů, který zajistí neutrální cash-flow.

	1	2	3	4	5	6	7	8	9	10
	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031
Provozní výdaje projektu * (včetně výdajů na údržbu a reinvestice)	0	0	150 000	1 500 000	1 500 000	1 500 000	1 500 000	1 500 000	1 500 000	1 500 000
Příjmy plynoucí z provozu projektu	0	0	0	0	0	0	0	0	0	0

Finanční cash-flow	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031
Příjmy – rozpočet žadatele	0	0	0	1 500 000	1 500 000	1 500 000	1 500 000	1 500 000	1 500 000	1 500 000
Příjmy – dotace	0	0	0	41 375 325	0	0	0	0		
Příjmy z provozu (tržby)	0	0	0	0	0	0	0	0		
Celkem příjmy:	**0**	**0**		**42 875 325**	**1 500 000**	**1 500 000**	**1 500 000**	**1 500 000**	**1 500 000**	**1 500 000**
Náklady projektu	0			1 500 000	1 500 000	1 500 000	1 500 000	1 500 000	1 500 000	1 500 000

Investiční (včetně nezpůsobilé DPH)	610 597	0	46 341 515	0	0	0	0	0		
Neinvestiční			2 990 691	0	0	0	0	0		
Provozní náklady	0	0	150 000	1 500 000	1 500 000	1 500 000	1 500 000	1 500 000	1 500 000	1 500 000
Celkem výdaje:	**610 597**	**0**	**49 482 205**	**1 500 000**	**1 500 000**	**1 500 000**	**1 500 000**	**1 500 000**	**1 500 000**	**1 500 000**
Roční cash flow:	**-610 597**	**0**	**-- 49 482 205**	**41 375 325**	**0**	**0**	**0**	**0**	**0**	**0**

Finanční plán pro variantní řešení projektu

Není relevantní.PŘÍLOHA Č. 1 ANALÝZA A ŘÍZENÍ RIZIK

Druh rizika a fáze projektu, ve které je možné riziko očekávat	Závažnost rizika (1 – nejnižší, 5 – nejvyšší)	Pravděpodobnost výskytu/četnost výskytu rizika	Předcházení/eliminace rizika
Technická rizika			
Nedostatky v projektové dokumentaci	3	2	PD pečlivě připravena ve spolupráci s ICT oddělením nemocnice, V případě potřeby bude řešeno v souladu s pravidly dotace.
Dodatečné změny požadavků investora	3	2	Projekt tvořen na základě požadavků managementu žadatele přímo ICT oddělením nemocnice. V případě potřeby bude řešeno v souladu s pravidly dotace.
Nedostatečná koordinace programátorských prací	2	2	Projekt koordinován osobami s dlouholetými zkušenostmi s managementem i v IT. V případě potřeby bude řešeno úpravou složení projektového týmu.
Výběr nekvalitního dodavatele	3	2	Výběr dodavatele bude organizován interním oddělením nemocnice / externí dodavatelskou firmou s dlouhodobými zkušenostmi v dané oblasti. V případě potřeby bude řešeno s ohledem na charakter problému v souladu se zákony a pravidly pro výběr dodavatele.
Nedodržené termínu realizace	2	2	V harmonogramu stanoven dostatečný časový limit, realizace projektu není časově náročná. V případě potřeby budou změny dopředu oznámeny v souladu s pravidly výzvy dotačního titulu.
Živelné pohromy	3	1	Nepředpokládá se. Předmětem projektu je přímo zajištění dat v případě nepředvídaných událostí. V průběhu projektu bude využíváno zálohování. V případě potřeby bude řešeno v souladu s podmínkami dotace a aktuálním problémovým stavem a jeho naléhavostí.
Zvýšení cen vstupů	3	2	Uvedené zohledněno při tvorbě zadávacích podmínek pro výběr dodavatele, bude ošetřeno ve smlouvě o dílo. V případě potřeby řešeno s ohledem na relevantní dokumentaci výběrového řízení a pokyny dotace.

Druh rizika a fáze projektu, ve které je možné riziko očekávat	Závažnost rizika (1 – nejnižší, 5 – nejvyšší)	Pravděpodobnost výskytu/četnost výskytu rizika	Předcházení/eliminace rizika
Nekvalitní projektový tým	3	1	Nepředpokládá se, členové projektového týmu mají dlouhodobé znalosti a zkušenosti v dané oblasti svých rolí. V případě potřeby bude řešeno personálními změnami.
Finanční rizika			
Neobdržení dotace	3	2	V případě neobdržení dotace bude projekt realizován s ohledem na disponibilitu vlastních zdrojů žadatele v podstatně delším časovém horizontu.
Nedostatek finančních prostředků na předfinancování a v průběhu realizace projektu	3	2	Finanční prostředky na předfinancování a kofinancování projektu jsou zajištěny. V případě potřeby by bylo řešeno okamžitě, pravděpodobně formou úvěru.
Právní rizika			
Nedodržení pokynů pro zadávání VZ	3	1	Nepředpokládá se, výběr dodavatele budou mít na starosti osoby s dlouhodobými znalostmi a zkušenostmi v dané oblasti. V případě potřeby bude okamžitě řešeno s ohledem na charakter nedodrženého.
Nedodržení podmínek IROP	3	2	Nepředpokládá se, žádost o dotaci připravuje externí společnost s dlouhodobými znalostmi v dané oblasti. V případě potřeby bude okamžitě řešeno s ohledem na charakter věci.
Nedodržení právních norem ČR, EU	3	2	Nepředpokládá se, jednotlivé části projektu jsou připravovány týmem osob s dlouhodobými znalostmi a zkušenostmi včetně právních. V případě potřeby bude okamžitě řešeno relevantními členy projektového týmu.
Nevyřešené vlastnické vztahy	3	1	Vlastnické vztahy jsou dlouhodobě neměnné a neuvažuje se s jejich změnami. V případě potřeby by bylo okamžitě řešeno ve spolupráci s managementem společnosti.

Druh rizika a fáze projektu, ve které je možné riziko očekávat	Závažnost rizika (1 – nejnižší, 5 – nejvyšší)	Pravděpodobnost výskytu/četnost výskytu rizika	Předcházení/eliminace rizika
Provozní rizika			
Neplnění dodavatelských smluv	3	2	Dodavatelské smlouvy budou obsahovat sankce vyplývající z jejich neplnění. V případě potřeby bude řešeno relevantními členy projektového týmu v souladu s pravily dotace a zákony.
Nedodržení indikátorů	3	1	Nepředpokládá se, indikátor stanoven v souladu s podmínkami výzvy. V případě potřeby bude řešeno zpracovatelem žádosti.
Nedostatek finančních prostředků v provozní fázi projektu	3	2	Nepředpokládá se. Žadatel si je vědom nezbytnosti realizovaného projektu i nákladů na zajištění provozu, s kterými je kalkulováno i v dalších letech po ukončení realizace. V případě potřeby bude řešeno s ekonomickým oddělením žadatele či managementem společnosti.