INTEGROVANÝ REGIONÁLNÍ OPERAČNÍ PROGRAM

2021–2027

SPECIFICKÁ PRAVIDLA PRO ŽADATELE A PŘÍJEMCE

STUDIE PROVEDITELNOSTI

SPECIFICKÝ CÍL 1.1

OBSAH

1. ÚVODNÍ INFORMACE O ZPRACOVATELI STUDIE PROVEDITELNOSTI

Obchodní jméno, sídlo, IČO a DIČ zpracovatele	Plus Projekt, s.r.o., Dostálova 97/5, Stránice, 602 00 Brno, 08671427, CZ08671427
Členové zpracovatelského týmu, jejich role a kontakty	Zpracovatelé studie: Mgr. Lenka Weiterová, Ph.D weiterova@plusprojekt.cz tel.:
Datum vypracování	8/2022

2. ZÁKLADNÍ INFORMACE O ŽADATELI

Obchodní jméno, sídlo, IČO a DIČ žadatele	Fakultní nemocnice Brno, Jihlavská 340/20, 625 00 Brno, 65269705, CZ65269705
Jméno, příjmení a kontakt na statutárního zástupce	MUDr. Ivo Rovný, 532 232 000, reditelstvi@fnbrno.cz
Jméno, příjmení a kontakt na kontaktní osobu pro projekt	Michal Plesar, Plesar.Michal@fnbrno.cz, tel.: 532 232 845
Nárok na odpočet DPH na vstupu ve vztahu ke způsobilým výdajům projektu (Ano x Ne)	NE

3. CHARAKTERISTIKA PROJEKTU A JEHO SOULAD S PROGRAMEM

Název projektu	Zvýšení fyzické kybernetické bezpečnosti FN Brno
Informace o podpořeném zařízení/subjektu (Obchodní jméno, sídlo, IČO)	Nerelevantní. Subjekt je žadatelem.
Místo realizace projektu	Město Brno
Popis cílů projektu	Cílem tohoto projektu je zvýšení úrovně kybernetické bezpečnosti informačních systémů nemocnice prostřednictvím pořízení modulárního datacentra. Technické opatření navrhované tímto projektem přispěje k předcházení hrozeb kybernetických a bezpečnostních incidentů. Výsledkem projektu tedy bude posílení ochrany informačních

	a komunikačních systémů žadatele před kybernetickými útoky. V rámci projektu bude technické opatření zabezpečeno v rámci 1 aktivity: Kontejnerová serverovna. Podporovanou aktivitou této výzvy je kybernetická bezpečnost. Cíle projektu tuto aktivitu naplňují.
Cílové skupiny projektu	Občané Vlivem realizace projektu nebudou ohroženy systémy provozované FNB, které zpracovávají osobní a citlivá data občanů ČR coby pacientů a klientů služeb zdravotní péče poskytované FNB. Bude tak zajištěna dostupnost a integrita těchto údajů. Cizinci Vlivem realizace projektu nebudou ohroženy systémy provozované FNB, které zpracovávají osobní a citlivá data občanů ČR coby pacientů a klientů služeb zdravotní péče poskytované FNB. Bude tak zajištěna dostupnost a integrita těchto údajů. Bude také zabezpečena dostupnost zdravotních služeb pro cizince, a to prostřednictvím ochrany informačního systému nemocnice před kybernetickými útoky. ~~Zaměstnanci ve veřejné zprávě~~ ~~Z pohledu zaměstnanců veřejné správy tvoří cílovou skupinu zaměstnanci FNB a dalších zdravotnických organizací (sdílení dat s dalšími subjekty, kde bude/byl pacient ošetřován). Jedná se o lékaře a ostatní vysokoškolský personál, střední a odborný zdravotnický personál, management nemocnice, studenty lékařských fakult, IT specialisty a ekonomičtí a administrativní pracovníky.~~ Všem těmto zaměstnancům přináší projekt vyšší dostupnost, bezpečnost a integritu informací prostřednictvím zabezpečení vybraných IS FNB. Projekt mj. zajišťuje, aby se zaměstnanci FNB dostali včas a spolehlivě k informacím služeb e−Governmentu (správa dat o pacientech apod.), které dále zpracovávají. ~~Zaměstnancům ostatních orgánů veřejné moci projekt přináší bezpečnější a dostupnější využívání elektronických služeb (výměna dat mezi různými zdravotnickými zařízeními apod.), které FNB poskytuje.~~
Popis vazeb na realizované či plánované projekty	Projekt má vazby na plánované projekty, které žadatel bude předkládat ve vyhlášené výzvě č. 4. Jedná se o projekty:

	- Zvýšení kybernetické bezpečnosti FN Brno II, jehož cílem je zvýšení kybernetické bezpečnosti a snížení rizika narušení nebo odcizení citlivých dat a údajů, zajištění, aby zaměstnanci pracovali s bezpečnými informačními systémy a aby byly prostřednictvím systémů poskytovány kvalitní a bezpečné služby. Tento projekt a další předkládaný projekt, zabezpečí vyšší a komplexnější míru bezpečnosti. Projekty jsou na sobě nezávislé a každé řešení přispívá ke zvýšení kybernetické bezpečnosti informačních systémů. - Modernizace bezdrátové síťové infrastruktury, jejichž cílem je zvýšení úrovně kybernetické bezpečnosti informačních systémů nemocnice prostřednictvím výměny přístupových bodů bezdrátové sítě. Tento projekt a další předkládané projekty zabezpečí vyšší a komplexnější míru bezpečnosti. Projekty jsou na sobě nezávislé a každé řešení přispívá ke zvýšení kybernetické bezpečnosti informačních systémů. - Projekt navazuje na realizaci projektu ve výzvě 10, jehož předmětem bylo zvýšení zabezpečení ISZS FNB prostřednictvím naplnění 6 technických opatření dle ZoKB. Jmenovitě došlo ke zvýšení ochrany integrity komunikačních sítí, zlepšení ověřování identity uživatelů. Dále byly zaváděny nástroje pro detekci kybernetických bezpečnostních událostí a pro sběr a vyhodnocení kybernetických bezpečnostních událostí. Došlo také ke zvýšení aplikační bezpečnosti a k zavedení nástroje pro zajišťování úrovně dostupnosti informací.

4. PODROBNÝ POPIS PROJEKTU

4.1 PODROBNÝ POPIS VÝCHOZÍHO STAVU

Fakultní nemocnice Brno je druhá největší nemocnice v České republice a zároveň nemocnice evropského významu, když ročně ošetří cca milion pacientů. Péči zajišťuje nejen pro obyvatele Brna a Jihomoravského kraje, ale i pro pacienty z Vysočiny, Zlínského a Olomouckého kraje. Pacientům všech věkových kategorií poskytuje specializovanou a super specializovanou péči ve všech oborech medicíny v souladu s dostupnými poznatky současné lékařské vědy.

FN Brno tvoří tři pracoviště: Pracoviště medicíny dospělého věku s areálem v Brně-Bohunicích na Jihlavské ulici, Pracoviště dětské medicíny s areálem v Černých Polích (Dětská nemocnice) a Pracoviště reprodukční medicíny na Obilním trhu (Porodnice). V jejich rámci pracují desítky specializovaných odborných klinik, ústavů, center a laboratoří.

V nemocnici pracuje cca 5700 zaměstnanců.

FN Brno byla rozhodnutím Národního úřadu pro kybernetickou a informační bezpečnost (dále také jen „**NÚKIB**“) ze dne 23. 10. 2018 dle § 22a zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „**ZKB**“), určena provozovatelem základní služby. K určení FN Brno provozovatelem základní služby došlo v důsledku naplnění kritérií stanovených vyhláškou č. 437/2017 Sb. o kritériích pro určení provozovatele základní služby (odvětvová kritéria 5. Zdravotnictví, druh služby 5.1. Poskytování zdravotních služeb).

Prostředí FN Brno je situováno z hlediska ICT infrastruktury do čtyř lokalit:

- areál Bohunice, Jihlavská 20, Brno;
- areál Porodnice, Obilní trh 11, Brno;
- areál Dětská nemocnice, Černopolní 9, Brno;
- transfuzní stanice Purkyňovo náměstí 2, Třebíč.

ICT infrastruktura FN Brno má následující parametry:

Parametr	Hodnota parametru	Poznámka
Počet informačních systémů základní služby identifikovaných dle ZKB	25	
Přibližný počet IP adres	8000	
Počet zdravotnických prostředků na síti (max. hodnota)	600	
Počet pevných PC	2500	
Počet virtuálních PC	1000	
Počet zaměstnanců celkem	5700	
Počet uživatelů v síti celkem	8900	Uživatele s pracovní smlouvou, cca 240 firemních účtů
Orientační počet switchů	300	
Orientační počet routerů	10	
Orientační počet WiFi AP	750	
Počet VPN gateway	3	
Počet firewallů samostatných	2	Zapojeno v HA
Počet Radius serverů	8	
Orientační počet Windows serverů	180	
Orientační počet Linux serverů	120	
Orientační počet databázových serverů	21	

Tabulka č.1 ICT infrastruktura FN Brno má následující parametry:

V březnu 2020, v době vyhlášení nouzového stavu kvůli šíření koronaviru, zasáhl FN Brno rozsáhlý kybernetický útok, který způsobil výpadky velké části ICT systémů a FN Brno přišla nenávratně o některá data, především o velké množství organizačních dat, podkladů pro veřejné zakázky či vědeckých podkladů.

Podle mluvčího brněnského krajského státního zastupitelství byla předběžně vyčíslená škoda více než 150 milionů korun. Šlo o největší incident svého druhu v Česku.

Po tomto rozsáhlém kybernetickém útoku se podařilo urychleně modernizovat centrální, páteřní switche a do konce roku 2020 se podařilo zrealizovat zakázku na modernizaci hlavního Firewallu.

V roce 2021 začala realizace veřejných zakázek, jejichž předmětem byla jednotlivá technická bezpečnostní opatření dle ZKB, a to z dotačního programu IROP výzvy č.10. FN Brno se rovněž zaměřila na budování organizačních bezpečnostních opatření, jako je např. budování a rozvoj interního týmu kybernetické bezpečnosti, navázání spolupráce s CSIRT týmem Masarykovy univerzity, jakož i na provedení analýzy rizik dle vyhlášky č. 82/2018 Sb. o o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „**VKB**“).

4.2 POPIS JEDNOTLIVÝCH ČÁSTÍ PROJEKTU

Stanovený rozsah SŘBI FN Brno

FN Brno v souladu s interním dokumentem **V_03 – Rozsah Systému řízení bezpečnosti informací FN Brno**, provedla identifikaci všech IS splňujících kritéria informačního systému základní služby (dále jen „**ISZS**“) a tím stanovila základ rozsahu systému řízení bezpečnosti informací (dále jen „**SŘBI**“) ve FN Brno, kdy je tento rozsah SŘBI pravidelně aktualizován v souladu s požadavky optimalizačního PDCA cyklu.

Rozsah celého SŘBI je tak definován veškerým technickým vybavením, komunikačními prostředky, programovým vybavením, objekty, které podporují ISZS, jakož i zaměstnanci a dodavateli, kteří podporují ISZS, včetně zdravotnických prostředků podporovaných ISZS. Do rozsahu řízení bezpečnosti informací standardně spadají všechna aktiva určeného systému a také další aktiva, u nichž je to s ohledem na bezpečnost systému žádoucí. Do SŘBI také spadá takový průmyslový, řídicí a obdobný specifický systém, který naplňuje kritéria definovaná v tomto, výše uvedeném, dokumentu.

Seznam ISZS v rozsahu SŘBI platný při provádění analýzy rizik:

ID ISZS	Název systému
ISZS01	**AMIS*H**
ISZS02	**AMIS*HD**
ISZS03	**FaRMIS**
ISZS04	**Intersystems Caché Ensamble**
ISZS05	**Laboratorní informační systém - Infolab**
ISZS06	**Laboratorní informační systém - Orpheus**
ISZS07	**MARIE PACS**
ISZS08	**RIS eMED Solution**

ISZS09	**Tranfúzní informační systém**
ISZS10	**Microsoft Dynamics NAV - Modul Stravovací provoz**
ISZS11	**ISP Concerto VM**
ISZS12	**Microsoft Dynamics NAV - Modul interní lékárna**
ISZS13	**IntelliSpace Philips - Perinatal**
ISZS14	**AW server**
ISZS15	**Syngo.Via Dětská nemocnice**
ISZS16	**Vigilant Sentinel**
ISZS17	**Space OnlineSuite**
ISZS18	**AQURE Enterprise**
ISZS19	**Lucia FISH**
ISZS20	**TruScan**
ISZS21	**EEG přístroj Walter PL-231**
ISZS22	**CobasIT1000**
ISZS23	**MicroMedic**
ISZS24	**CobasITMiddleware**
ISZS25	**Syngo.Via Bohunice**

Tabulka č. 2 Seznam ISZS v rozsahu SŘBI platný při provádění analýzy rizik:

Návrh bezpečnostních opatření

FN Brno provedla v roce 2022 analýzu rizik v souladu s dokumentem **KB_P_24_M01 Metodika pro identifikaci aktiv a hodnocení rizik**, výsledkem, které je seznam zranitelností, u nichž se při hodnocení rizik vyskytla nejvyšší hodnota míry rizika.

Na základě těchto výsledků byl zpracován **Plán zvládání rizik**, ze kterého byly vybrány technická bezpečnostní opatření pro tento projekt:

Položka	**Plnění technického bezpečnostního opatření**
Kontejnerová serverovna	§ 17 Fyzická bezpečnost

ID opatření:	*1*
Oblast opatření podle ZKB a vyhlášky o kybernetické bezpečnosti:	*Oblast opatření podle vyhlášky o kybernetické bezpečnosti: § 17 Fyzická bezpečnost*
Název opatření:	*Kontejnerová serverovna*
KII/VIS/ISZS/IS/KS:	*Opatření se týká všech ISZS určených v rozsahu SŘBI*
Popis opatření:	*V projektu se předpokládá pořízení Datového centra ve formě kontejnerového řešení, které bude zahrnovat veškeré požadavky na odpovídající úroveň fyzické bezpečnosti, tzn. řešení včetně serverových racků, kompletní elektroinstalace včetně chytré kabeláže pro propojení jednotlivých technologií, dimenzovaných záložních zdrojů, hasebního systému, systému chlazení. Na straně FN Brno to bude zajistit provedení souvisejících drobných stavebních úprav na určeném místě, propojení na napájecí infrastrukturu Motorgenerátorů a připojení kompletní síťové infrastruktury. Kontejnerové Datové centrum bude sloužit jako trvale bezobslužné pracoviště provozované 7x24x365. Veškerá technologická infrastruktura musí být nainstalována uvnitř kontejneru a nebude přesahovat mimo jeho okraje. Kontejnerové Datové centrum musí mít oddělená vstupní komora kontejneru od datového sálu, kapacita datových stojanů (racků) v kontejneru musí být minimálně 12 ks (42U x minimálně 1000 x 600 mm) a průměrná výkonová hustota minimálně 5 kW / rack.*
Sdílení opatření se ISOUI:	~~*Technické opatření bude zabezpečovat celý interní bezpečnostní perimetr fyzické bezpečnosti umístěním podpůrných technických aktiv zajišťujících provoz ISZS z rozsahu SŘBI do bezpečného datového centra*~~

1. Kontejnerová serverovna

V současnosti disponuje FN Brno dvěma Datovými centry umístěnými v lokalitě Bohunice. Pracovníci NÚKIB provedli osobní kontrolu a posouzení stavu obou Datových center. První Datové centrum je moderní splňující všechny požadavky na zajištění provozních podmínek a odpovídající fyzické bezpečnosti. Toto Datové centrum také disponuje certifikací TIER III dle Uptime Institute.

Druhé Datové centrum, které je starší, nesplňuje požadavky na zajištění odpovídající míry kybernetické bezpečnosti i přes všechna opatření. Tuto skutečnosti konstatovali i pracovníci NÚKIB, kteří hodnotili toto druhé Datové centrum jako nevyhovující. Hlavní problém tohoto Datového centra je, že ve vestavěné jako další místnost do kancelářských prostor Centra Informatiky, kdy stěny tohoto Datového centra jsou běžné sádrokartonové příčky a vstup tvoří běžné interiérové protipožární dveře a existují další faktické nedostatky vyplývající z tohoto řešení.

FN Brno také nedisponuje objektem, který by bylo možné jednoduše stavebně připravit pro potřeby bezpečného a moderního Datového centra, které bude parametry shodné s prvním Datovým centrem, tj ve standardu na úrovni TIER III dle Uptime Institute.

Jako optimální řešení z hlediska možností FN Brno vyšlo pořízení Datového centra ve formě kontejnerového řešení, které bude zahrnovat veškeré požadavky na odpovídající úroveň fyzické bezpečnosti, tzn. řešení včetně serverových racků, kompletní elektroinstalace včetně chytré kabeláže pro propojení jednotlivých technologií, dimenzovaných záložních zdrojů, hasebního systému, systému chlazení. Na straně FN Brno to bude zajistit provedení souvisejících drobných stavebních úprav na určeném místě, propojení na napájecí infrastrukturu Motorgenerátorů a připojení kompletní síťové infrastruktury. Kontejnerové Datové centrum bude sloužit jako trvale bezobslužné pracoviště provozované 7x24x365. Veškerá technologická infrastruktura musí být nainstalována uvnitř kontejneru a nebude přesahovat mimo jeho okraje. Výjimkou mohou být chladicí jednotky, které budou umístěny buď na střeše kontejneru anebo mimo kontejner.

Požadavky na řešení

- Oddělená vstupní komora kontejneru od datového sálu
- Počet datových stojanů (racků) v kontejneru 12 ks (42U x minimálně 1000 x 600 mm)
- Průměrná výkonová hustota minimálně 5 kW / rack
- Klasifikace Tier: TIER III
- Chlazeni musí být na bázi nepřímého free – coolingu, který bude schopen zajistit konstantní podmínky pro ICT včetně ztrát a tepelných zisků. Systém free-coolingu musí výkonem pokrýt veškeré tepelné zisky (výkon ICT, ztráty UPS, tepelné zisku z exteriéru, ztráty osvětlení a jiných technologií
- Veškeré technologie budou integrované uvnitř kontejneru s výjimkou externích chladících jednotek
- Kontejner bude vybaven samočinným hasicím zařízením SHZ (inertní plyn).
- Fyzická bezpečnost bude tvořena samotným skeletem kontejneru s plášťovou a prostorovou ochranou pomocí EZS a CCTV s napojením na operační centrum

- Řízení vstupu do vstupní části kontejneru bude řešeno přístupovým systémem ACS zahrnujícím bezkontaktní čtečku karet napojenou na systém FM Brno
- Kamerový systém s napojením na operační centrum včetně identifikace vstupujícího
- Součástí kontejneru je strukturovaná kabeláž podle standardů FN Brno
- Musí být umožněn monitoring environmentální a monitoring fyzické vrstvy kabeláže
- Veškeré technologie budou integrované uvnitř kontejneru s výjimkou motorgenerátorů a externích chladících jednotek

Plnění bezpečnostního opatření: **§ 17 Fyzická bezpečnost**

4.3 ODŮVODNĚNÍ POTŘEBNOSTI A ÚČELNOSTI INVESTICE

- stručné zdůvodnění projektu;

Projekt reaguje na potřebu zvýšení kybernetické bezpečnosti Fakultní nemocnice Brno, kdy se nemocnice v minulosti stala terčem kybernetického útoku. V současnosti disponuje FN Brno dvěma Datovými centry umístěnými v lokalitě Bohunice. Pracovníci NÚKIB provedli osobní kontrolu a posouzení stavu obou Datových center. První Datové centrum je moderní splňující všechny požadavky na zajištění provozních podmínek a odpovídající fyzické bezpečnosti. Toto Datové centrum také disponuje certifikací TIER III dle Uptime Institute. Druhé Datové centrum, které je starší, nesplňuje požadavky na zajištění odpovídající míry kybernetické bezpečnosti i přes všechna opatření. Tuto skutečnosti konstatovali i pracovníci NÚKIB, kteří hodnotili toto druhé Datové centrum jako nevyhovující. FN Brno provedla v roce 2022 analýzu rizik v souladu s dokumentem KB_P_24_M01 Metodika pro identifikaci aktiv a hodnocení rizik, výsledkem, které je seznam zranitelností, u nichž se při hodnocení rizik vyskytla nejvyšší hodnota míry rizika. Na základě těchto výsledků byl zpracován Plán zvládání rizik, ze kterého byly vybrány technické bezpečnostní opatření pro tento projekt. Podrobněji stávající stav popisuje subkapitola 4.1 a 4.2.

- vazba projektu na specifický cíl 1.1 a výzvu:

Projekt je plně v souladu s vyhlášenou výzvou č. 4 „*Kybernetická bezpečnost*“ pro přechodové regiony a SC 1.1 „*Využívání přínosů digitalizace pro občany, podniky, výzkumné organizace a veřejné orgány*,“ kde jednou z podporovaných aktivit je právě kybernetická bezpečnost. Projektem je řešena realizace technických bezpečnostních opatření podle § 5 odst. 3 zákona o kybernetické bezpečnosti. Fakultní nemocnice Brno spadá mezi oprávněné žadatele, jedná se organizaci zřízenou Ministerstvem zdravotnictví ČR.

- identifikace dopadů a přínosů projektu s důrazem na popis dopadů na cílové skupiny;

Vlivem realizace projektu nebudou ohroženy systémy provozované FNB před kybernetickými útoky, které zpracovávají osobní a citlivá data občanů ČR coby pacientů a klientů služeb zdravotní péče poskytované FNB. Bude tak zajištěna dostupnost a integrita těchto údajů. ~~Projekt přináší vyšší dostupnost, bezpečnost a integrit informací prostřednictvím zabezpečení vybraných IS FNB a to zaměstnancům FNB jakož to zaměstnancům ve veřejné správě.~~ Projekt zabezpečí dostupnost kvalitních zdravotnických služeb v potřebné kapacitě a v potřebném čase pro své klienty, tj. občany ČR, cizince, a to prostřednictvím ochrany informačního systému nemocnice před kyberútoky. Projekt taktéž zabezpečí stabilní pracovní IT prostředí pro zaměstnance nemocnice.

- zdůvodnění potřebnosti pořizovaného vybavení/majetku (jeho počtu, umístění a zdůvodnění využití v souladu s výzvou);

Projekt je zaměřen na zavedení mechanizmů, které výrazným způsobem zvyšují úroveň kybernetické bezpečnosti ICT infrastruktury a tím jednotlivých informačních systémů základní služby FN Brno.

S ohledem na provedenou analýzu rizik a zpracovaný Plán zvládání rizik, byly vybrány technická bezpečnostní opatření pro tento projekt:

Položka	**Plnění technického bezpečnostního opatření**
Kontejnerová serverovna	§ 17 Fyzická bezpečnost

Implementace technologií ve zmíněných oblastech přinese výrazné zvýšení současného stavu kybernetické bezpečnosti ve FN Brno a naplnění souladu se ZKB. Pro dosáhnutí cíle je nutné implementovat nezbytně nutné vybavení, ať už na úrovni HW či SW zajišťující jednotlivá technická opatření popsaná blíže kapitole 4.2. ve vazbě na konkrétní paragrafy (§ 17-§ 28) VKB 82/2018 Sb.

Vzhledem k harmonogramu projektu, kdy se počítá s realizací veřejné zakázky v průběhu roku 2023, bude detailní analýza konkrétních požadavků na zajištění technologií pro jednotlivá technická opatření provedena v rámci přípravy na VZ. Pořízený majetek HW bude umístěn v areálu FN Brno areál Bohunice, Jihlavská 20, Brno.

- popis souladu projektu s **Prováděcím dokumentem programu Digitální Česko pro čerpání z IROP 2021-2027;**

Předkládaný záměr a jím navrhovaná opatření jsou v souladu s **Prováděcím dokumentem programu Digitální Česko pro čerpání z IROP 2021-2027,** konkrétně s těmito vybranými technickými opatřeními v něm uvedenými:

  - fyzická bezpečnost

- zdůvodnění potřebnosti stavby, přístavby, nástavby a stavebních úprav (rekonstrukce, modernizace);

Projekt neřeší žádné stavební úpravy objektu, jedná se pouze o soubor dodávek hmotného a nehmotného majetku, příp. Modernizace bezdrátové síťové infrastruktury

- popište možnosti alternativních řešení:

Varianta 1 – Nulová varianta

Při nulové variantě nebude FNB kybernetickou bezpečnost vůbec dále rozvíjet. Nulová varianta povede k tomu, že nemocnice nebude připravena na kybernetické hrozby. Potenciálním důsledkem je neschopnost péče o pacienty a neposkytování základní služby v oblasti zdravotnictví. Nebude plnit zákonné povinnosti.

Varianta 2 – Provozní varianta

Při zachování současného stavu nebude FNB dostatečně připravena na kybernetické bezpečnostní incidenty a na jejich předcházení. Bez nastavení a definování procesů bezpečnostní politiky nelze zajistit ochranu příslušných aktiv. V případě bezpečnostního incidentu tak bude nemocnice vystavena opakování dřívějších zkušeností s dopadem velkého rozsahu, včetně poškození důležitých aplikací informačního systému a odcizení dat. Nebude plnit zákonné povinnosti.

Varianta 3 – Rozvojová varianta

Realizací projektu dojde k odstranění některých z nejpalčivějších problémů kybernetické bezpečnosti FNB. Cílový stav počítá s kvalitně provedenými opatřeními, která budou součástí většího celku a přispějí k větší bezpečnosti informačního systému a jednotlivých aplikací a snížení rizika výskytu bezpečnostních incidentů. Díky realizaci projektu bude významně omezen dopad poškození informačních systému, případně odcizení dat, a to i za běžného provozu.

Fakultní nemocnice Brno preferuje třetí, tedy rozvojovou variantu.

4.4 HARMONOGRAM realizace projektu

Celkový průběh prací posloupnou návazností jednotlivých aktivit prezentuje Ganttův diagram, přiložen je také tradiční harmonogram.

Přípravná fáze projektu započala v dubnu 2022 zpracováním Projektového záměru pro odsouhlasení zřizovateli a specifikací aktivit v rámci kybernetické bezpečnosti. Vybraný dodavatel následně zpracoval Žádost o dotaci a podklady pro vydání Stanoviska Hlavního architekta eGovernmentu. Po podání žádosti bude následovat hodnotící proces v uvažované délce cca 2-3 měsíce. Souběžně s hodnotícím procesem lze přejít k realizaci zadávacích a výběrových řízení na jednotlivé VZ, vč. projednání a schválení v orgánech zřizovatele. Na vlastní dodávku vybavení, techniky, SW vč. implementace byla stanovena doba 15 měsíců s tím, že se u většiny dodávek předpokládá průběžné a paralelní plnění. Předpokládá se, že by dotační projekt s vybranými aktivitami podporujícími kybernetickou bezpečnost mohl být ukončen v říjnu roku 2024.

Činnost	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10
	22									23												24									
Přípravná fáze																															
Projektový záměr																															
Výběr aktivit pro žádost o dotaci IROP vč. výběru odborného zpracovatele																															
Žádost o dotaci IROP																															
Hodnocení žádosti o dotaci																															
Uzavření právního aktu/smlouvy o poskytnutí podpory																															
Realizační fáze																															
Příprava zadávacích podmínek dodavatelé prvků/aktivit KB																															
Realizační management (administrace projektu s poskytovatelem dotace)																															
Zpracování Zpráv o realizaci projektu a žádostí o platbu																															
VŘ na dodavatele prvků/aktivit KB																															
Vlastní dodávka technologií, vybavení, SW, aj. vč. implementace řešení																															
Zahájení provozu s implementovanými opatřeními zvyšujícími KB																															

Tabulka č. 3 Gantův diagram

Činnost	Předpoklad zahájení realizace	Předpoklad dokončení realizace
Přípravná fáze		
Projektový záměr	Duben 2022	Červen 2022
Výběr aktivit pro žádost o dotaci IROP vč. výběru odborného zpracovatele	Červen 2022	Červenec 2022
Žádost o dotaci IROP	Srpen 2022	Srpen 2022
Hodnocení žádosti o dotaci	Září 2022	Listopad 2022
Uzavření právního aktu/smlouvy o poskytnutí podpory	Listopad 2022	Prosinec 2022
Realizační fáze		
Příprava zadávacích podmínek dodavatelé prvků/aktivit KB	Listopad 2022	Prosinec 2022
Realizační management (administrace projektu s poskytovatelem dotace)	Leden 2023	Říjen 2024
VŘ na dodavatele prvků/aktivit KB	Únor 2023	Červen 2023
Vlastní dodávka technologií, vybavení, SW, aj. vč. implementace řešení	Červenec 2023	Říjen 2024
Zahájení provozu s implementovanými opatřeními zvyšujícími KB	1.11. 2024	x

Tabulka č. 4 Harmonogram projektu

4.5 PŘIPRAVENOST PROJEKTU K REALIZACI

- **Technická připravenost:**
  - <u>připravenost projektové dokumentace:</u>

    V rámci přípravy projektu byla FN Brno provedla v roce 2022 analýzu rizik v souladu s dokumentem KB_P_24_M01 Metodika pro identifikaci aktiv a hodnocení rizik, výsledkem, které je seznam zranitelností, u nichž se při hodnocení rizik vyskytla nejvyšší hodnota míry rizika. Tato bude dále

rozpracována do Technické projektové dokumentace se specifikací prvků/aktivit KB, a to po schválení financování projektu. Bude použita jako podklad k Zadávací dokumentaci pro Veřejné zakázky. Předpoklad zpracování je v období 11-12/2022

- připravenost dokumentace k zadávacím a výběrovým řízením, údaje o proběhlých řízeních, o uzavřených smlouvách;
  Příprava dokumentace k zadávacím a výběrovým řízením naváže na zpracování Technické dokumentace. Vyhlášení VZ a vlastní výběr dodavatele/ů bude realizován v termínu 02-06/2023.
- stav smluvního vztahu mezi objednatelem služeb a žadatelem:
  Objednatelem služeb a zároveň žadatelem je Fakultní nemocnice Brno
- stav závazných stanovisek dotčených orgánů státní správy:
  Předmětem projektu nejsou aktivity související se stavbou, není zde tedy třeba vyjádření státních správy.
  Pro aktivity e-Governmentu bylo zažádáno o Stanovisko útvaru Hlavního architekta e-Governmentu. Potvrzení o přijetí žádosti o vydání stanoviska je přiloženo k žádosti.
- informace o procesu vydání dokladů prokazujících povolení umístění stavby a dokladů prokazujících povolení k realizaci stavby dle zákona č. 183/2006 Sb., o územním plánování a stavebním řádu, ve znění pozdějších předpisů, pokud je pro projekt relevantní – popis procesu, termíny žádostí, nabytí právní moci:
  Předmětem projektu nejsou aktivity související se stavbou, tyto doklady jsou nerelevantní.

- **Finanční připravenost:**
  - způsob financování realizace projektu, popis zajištění předfinancování a spolufinancování projektu:
    Financování realizační části a provozní fáze bude zajištěno následovně:
    Předfinancování projektu odpovídající podílu ERDF (100%) je zajištěno v rozpočtové kapitole zřizovatele FN Brno, tj. MZ ČR. Náklady realizační fáze pak budou refundovány z prostředků dotace EU. V průběhu realizace projektu budou poskytovateli dotace předkládány Monitorovací zprávy spolu s Žádostmi o platbu.

    Provozní fáze bude hrazena z provozního rozpočtu žadatele.

- **Administrativní připravenost:**
  - zajištění administrativní kapacity – počet a kvalifikace osob, které budou řídit projekt v době jeho realizace;
    Za realizaci předkládaného projektu nese plnou odpovědnost žadatel o dotaci, kterým je Fakultní nemocnice Brno. Za účelem úspěšné realizace projektu sestavil žadatel projektový tým, jehož úkolem bude projektové řízení a realizace. Složení projektového týmu odpovídá významu a rozsahu projektu, přičemž je možné v případě potřeby rozšířit stávající projektový tým o interní či externí odborníky.

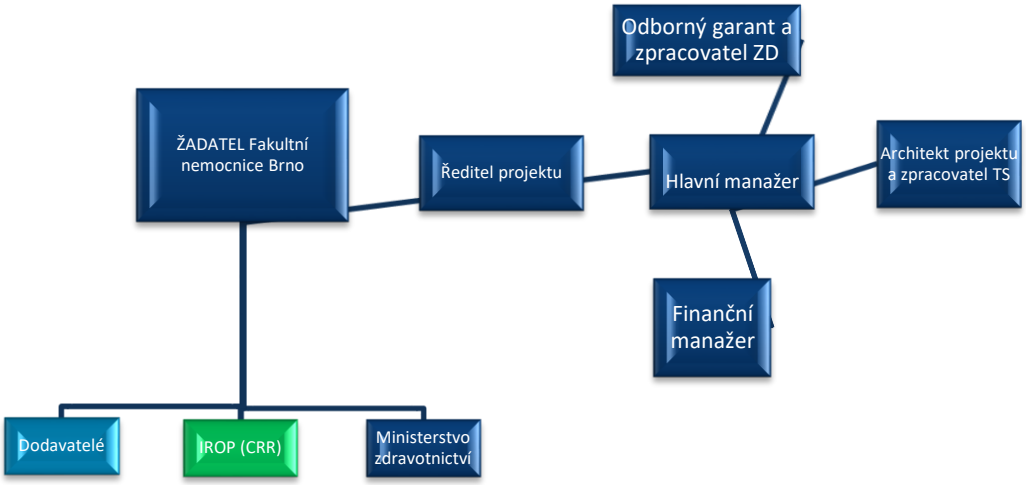
Zodpovědnou osobou za úspěšnou realizaci projektu je **Ředitel projektu** (Ing. Peter Mešťaník, náměstek pro informatiku), který je přímo podřízený žadateli a je nadřízený všem ostatním členům týmu. Je zodpovědný za realizaci a úspěch projektu vůči žadateli i zřizovateli. Vedoucí realizačního týmu bude řídit veškerou práci v týmu. Mezi jeho hlavní kompetence bude patřit řízení pracovníků zapojených do realizace projektu, řízení a monitorování procesů, bude tento projekt zastupovat navenek, zajišťovat potřebné zdroje, zlepšovat komunikaci v týmu a také tento tým motivovat.

Hlavní manažer (Michal Plesar, vedoucí Oddělení pro řízení projektů) je přímo podřízený Řediteli projektu, bude připravovat setkání týmu a vést o něm zápisy, udržovat projektovou dokumentaci, monitorovat realizaci projektu a podílet se na provedení výběrových řízení na dodavatele. Bude zajišťovat realizaci projektu v souladu s podmínkami stanovenými poskytovatelem dotace. Spolupracuje s řídícím orgánem. Účastní se průběžných a následných kontrol ze strany řídícího orgánu či vnějších nezávislých kontrol, vykonává kontrolu nad zpracováním Monitorovacího hlášení s žádostí o platbu/bez platby, Závěrečné monitorovací zprávy. Dále bude dohlížet na publicitu projektu.

Odborný garant a zpracovatel ZD (Robert Kotzian, Manažer kybernetické bezpečnosti) úzce spolupracuje s Hlavním manažerem projektu a je odpovědný za zajištění realizace technických podkladů, dohled při dodávce technologií, vybavení HW a SW, aj. vč. implementace řešení, komunikaci s dodavatelem a příslušnými institucemi. Jeho zodpovědnost je zajistit principy toku informací mezi dodavatelem TPD, dodavatelem dodávek a služeb a žadatelem, zajistit podmínky a součinnost jednotlivých oddělení a pracovníků. Z hlediska vnitřních vazeb týmu je odpovědný Hlavnímu manažerovi projektového týmu a má pravomoc delegovat jednotlivé úkoly na další členy týmu. Z pohledu vnějších vazeb má pravomoc jednat v rámci stanoveného harmonogramu jednotlivých fází projektu a jejich rozpočtu.

Architekt projektu a zpracovatel TS (Robert Schindler, architekt kybernetické bezpečnosti) bude zajišťovat realizaci projektu v souladu podmínkami pro kybernetickou bezpečnost. Podílí se na přípravě TPD, dále na zajištění implementace a následném provozu.

Finanční manažer (Ing. Robert Czékus, MHA, ekonomický náměstek) projektu nese odpovědnost za ekonomické ukazatele, za bezproblémové účetnictví a efektivní čerpání dotace. Jeho působení v projektu bude zahrnovat i kontrolu formální správnosti účetních dokladů, a za to pak ponese plnou zodpovědnost. Mezi další činnosti bude patřit příprava podkladů pro žádosti o platbu, kontrola čerpání rozpočtu a informování projektového manažera o stavu čerpání rozpočtu a finančních tocích a dále i případné zpracovávání návrhů na eventuální změny v rozpočtu.



Obrázek č. 1 Organizační struktura projektu (Zdroj: vlastní zpracování)

- popis organizačních a finančních vztahů mezi příjemcem podpory a provozovatelem v době realizace, pokud se liší provozovatel projektu od příjemce podpory:
  Příjemce podpory a provozovatel projektu je totožný – Fakultní nemocnice Brno.

4.6 EKONOMICKÁ/ NEEKONOMICKÁ ČINNOST ŽADATELE O PODPORU

Fakultní nemocnice Brno zajišťuje výkon veřejné správy v oblasti poskytování zdravotní péče na území Jihomoravského kraje pro svého zřizovatele (Ministerstvo zdravotnictví) v souladu s příslušnými právními předpisy a pokyny zřizovatele.

Poskytování zdravotní péče je hrazeno z veřejného zdravotního pojištění, případně z jiných veřejných zdrojů, výjimečně je hrazeno samoplátci v rámci jednotlivých zdravotnických výkonů.

Z uvedeného plyne, že Fakultní nemocnice Brno v její hlavní oblasti zajišťování zdravotní péče nevykonává ekonomickou činnost, tj. nenabízí zboží ani služby na trhu.

Projekt negeneruje žádné příjmy, tudíž se z finančního hlediska jedná o nenávratnou investici. Cílem projektu není přímé generování zisku, ale zvýšení kybernetické bezpečnosti informačních systémů. Hodnota investice je vyjádřena především její užitností a garantovaného poskytování zdravotní péče pro cílové skupiny projektu.

5. PROKÁZÁNÍ PRÁVNÍCH VZTAHŮ

V rámci projektu bude pořízen movitý majetek.

Do projektu vstupuje majetek v podobě prostor žadatele tj. nemovitý majetek. V rámci projektu nebudou realizovány aktivity vedoucí k investici do stávajícího nemovitého majetku. Tento nemovitý majetek bude dotčen realizací projetu tím, že zde bude umístěn pořízený movitý majetek v podobě hardware. Parcelní čísla jsou uvedena na ~~LV č. 9 k.ú. Starý Lískovec a~~ LV č. 10 k.ú. Bohunice - par. č. 3174 a 3156/1, které jsou přílohou žádosti.

Nemovitý a movitý majetek je ve vlastnictví Ministerstva zdravotnictví ČR, jakožto zřizovatele Fakultní nemocnice Brno. Nemocnice má ke všem movitým i nemovitým věcem právo hospodařit se svěřeným majetkem státu.

Nemovitá věc v katastrálním území „Budovy Fakultní nemocnice Brno – zastavěná plocha a nádvoří“	**Právní vztah**
~~LV č. 9 k.ú. Starý Lískovec~~	~~Právo hospodaření se svěřeným majetkem státu~~
LV č. 10 k.ú. Bohunice par. č. 3174 parc. č. 3156/1	Právo hospodaření se svěřeným majetkem státu

Tab. č. 5 Právní vztahy – nemovitý majetek

Movitá věc (*uvést výčet*)	**Právní vztah**
switche/routery/ ostatní síťové prvky	Právo hospodaření se svěřeným majetkem státu
rackové skříně	Právo hospodaření se svěřeným majetkem státu
datová centra	Právo hospodaření se svěřeným majetkem státu
kabeláž/propojky	Právo hospodaření se svěřeným majetkem státu
servery	Právo hospodaření se svěřeným majetkem státu

Tab. č. 6 Právní vztahy – movitý majetek

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

- Popis vlivů projektu na rovné příležitosti, rovnost pohlaví a zákaz diskriminace.

Rovné příležitosti a zákaz diskriminace

Předkládaný projekt respektuje dodržování rovných příležitostí a nediskriminace. Výstupy projektu budou jak na straně uživatelů/zaměstnanců/zodpovědných osob, tak na straně cílové skupiny (občané, cizinci využívající služeb Nemocnice) přístupné všem bez rozdílu pohlaví, rasy, etnického původu, náboženského vyznání, víry, zdravotního postižení, věku či sexuální orientace.

Projekt je z hlediska rovných příležitostí neutrální.

Rovnost pohlaví

Pracovní místa dotčená realizací projektu i výstupy projektu (pořizovaná infrastruktura pro zabezpečený nemocniční IS) budou dostupná všem bez ohledu na pohlaví.

Pracovní místa jsou obsazena a budou obsazována zaměstnanci, kteří splňují požadovanou kvalifikaci a jsou vhodná jak pro muže, tak pro ženy.

Princip rovnosti pohlaví u cílové skupiny je zajištěn samotnou povahou instituce – lékařského zdravotnického zařízení, které je určené k léčení lidí bez rozdílu pohlaví. Podle čl. 31 Listiny základních práv a má každý právo na ochranu zdraví a občané mají na základě veřejného pojištění právo na bezplatnou zdravotní péči.

Projekt je z hlediska rovnosti pohlaví neutrální.

6.2 SOULAD PROJEKTU S PRINCIPY UDRŽITELNÉHO ROZVOJE

- Popis souladu projektu s principy udržitelného rozvoje a popis vlivů projektu na životní prostředí:
    - Vlivy projektu na klima a vlivy klimatu na výstupy projektu

      Realizace projektu nebude mít negativní vliv na klima, klima nikterak neovlivní výstupy projektu. V rámci projektu budou pořizovány moderní technologie – HW a SW s minimální energetickou náročností. Nepředpokládá se tedy významný nárůst nepřímých emisí touto aktivitou.
      Vzhledem k povaze pořizovaných technologií se dle legislativy EK nevyžaduje výpočet uhlíkové stopy. Předkládaný projekt nepovede ke zvýšení emisí skleníkových plynů.
      Jedná se o infrastrukturu, která bude instalována v interních prostorách žadatele, takže klimatické změny nemají žádný vliv na její odolnost. Stejně tak neexistuje spojitost mezi vlivem klimatu na pořizovaný SW. Zajištění klimatické odolnosti je tedy v tomto případě irelevantní.

- Vlivy na udržitelné využívání a ochranu vodních zdrojů:
  Neočekává se, že činnost v rámci projektu poškodí dobrý stav nebo dobrý ekologický potenciál vodních útvarů, včetně povrchových a podzemních vod. Nejedná se o realizaci stavebních prací nebo jiných dodávek v rámci exteriéru Nemocnice.
  Pořizované technologie nebudou napojeny na vodovodní infrastrukturu, ani ji nebudou využívat pro dosažení plánovaných výstupů v rámci projektu. Realizace projektu nemá vliv na vodní zdroje.

- Opatření týkající se předcházení vzniku odpadů a recyklace:
  V rámci realizace aktivit projektu nebude docházet k produkci stavebního a demoličního odpadu, stavební práce nejsou pro zavedení pořizované infrastruktury uvažovány.
  Případný obalový materiál z pořízených technologií bude likvidován v souladu se zákonem o likvidaci odpadů dle zákonu č. 541/2020 Sb. Zákon o odpadech. V převážné většině se bude jednat o odpad z kategorie papír a plast. Životnost pořizované infrastruktury (HW) je cca 7 let. Likvidace pořizovaného zařízení po skončení životnosti bude probíhat standardně dle platných předpisů tak, aby byly dodrženy veškeré ekologické a bezpečnostní standardy a bylo zajištěno, že nedojde k případné kompromitaci dat.

- Opatření týkající se prevence a omezování znečištění ovzduší, vody nebo krajiny:
  Investice neobsahuje a nebude využívat nebezpečné látky a chemikálie a látky vzbuzující mimořádnou obavu dle REACH.
  Realizace podporovaných aktivit a pořizované infrastruktury vzhledem ke své povaze nepovede ke zvýšení emisí znečišťujících látek.

- Opatření na ochranu a obnovu biologické rozmanitosti a ekosystémů:
  Investice nespadají do působnosti hodnocení EIA, neovlivňují předměty ochrany přírody a krajiny, nejsou realizovány v chráněných územích a biodiverzitně hodnotných oblastech. Jedná se o aktivity směřující do vybavení technickou infrastrukturou v interiéru budov, které jsou v místě realizace provozovány již řadu let a jejich provoz splňuje všechny zákonem dané požadavky ve vztahu k ochraně území a životního prostředí.
  Realizací projektu tedy nebudou nikterak negativně ovlivněna zvláště chráněná území, soustavy Natura 2000, nedojde k poškození dobrého stavu a odolnosti ekosystémů nebo stanovišť, a zvláště chráněných druhů rostlin a živočichů.

7. VÝSTUPY A VÝSLEDKY PROJEKTU

Výstupem projektu bude 25 nových prvků k zajištění odpovídajících standardů kybernetické bezpečnosti.

Výstupy technických opatření

Výstupy aktivity č. 1 – Kontejnerová serverovna

- Bude pořízeno kontejnerové Datové centrum, které bude zahrnovat veškeré požadavky na odpovídající úroveň fyzické bezpečnosti, tzn. řešení včetně serverových racků, kompletní elektroinstalace včetně chytré kabeláže pro propojení jednotlivých technologií, dimenzovaných záložních zdrojů, hasebního systému, systému chlazení, tak aby cílově kompletně nahradilo nevyhovující Datové centrem DC-T.

- Popis plnění cílů projektu, resp. jak jednotlivé výstupy přispívají k plnění cílů projektů:

Výše uvedený výstup má za cíl zvýšení kybernetické bezpečnosti prostřednictvím pořízení modulárního datacentra. Datacentrum zajistí podporu provozu klíčových systémů nemocnice. Cílový stav poskytne potřebnou úroveň dostupnosti a důvěryhodnosti pro provozování nemocničních informačních systémů a zpracování pacientských údajů zaměstnanci. Výstupy projektu přispějí k předcházení hrozeb kybernetických a bezpečnostních incidentů.

Indikátory výstupu:

Název a kód indikátoru	Cílová hodnota	Popis stanovení cílové hodnoty
304 002 - Nové nebo modernizované prvky k zajištění standardů kybernetické bezpečnosti	25	Započítání všech projektem navržených technických opatření pro každý ISZS nemocnice zvlášť, detaily viz příloha žádosti o dotaci.

Tab. č. 7 Indikátory výstupu

Uveďte očekávané významné multiplikační efekty projektu:

Projekt je zaměřen na zavedení mechanizmů, které výrazným způsobem zvyšují bezpečnost informačních systémů Fakultní nemocnice Brno prostřednictvím pořízení modulárního datacentra. Realizaci projektu přinese významný posun v řízení komplexního Systému řízení bezpečnosti informací včetně reakce na kybernetické bezpečnostní události a zajistí tak rychlé řešení případných kybernetických útoků. Dále přinese výrazné ušetření časových možností specialistů, kteří se tak budou moci věnovat dalším rozvojovým aktivitám v oblasti kybernetické bezpečnosti. Jiné významné multiplikační efekty projektu nejsou očekávány.

9. ZAJIŠTĚNÍ UDRŽITELNOSTI PROJEKTU

- **Provozní**
  - popis využitelnosti pořizované investice;
    Po dobu životnosti/udržitelnosti bude pořizovaná investice (HW, SW včetně implementace) využívána pro zajištění účelu projektu - tj. pro zabezpečení kybernetické bezpečnosti Fakultní nemocnice Brno.

  - nakládání s majetkem pořízeným z dotace ve vlastnictví příjemce třetími osobami a partnery, předpokládané termíny změn;
    Pořízený majetek bude po celou dobu realizace i udržitelnosti projektu ve vlastnictví žadatele, resp. zřizovatele Ministerstvo zdravotnictví ČR. Fakultní nemocnice Brno má právo hospodaření se svěřeným majetkem. Není předpokládáno využití třetími osobami ani jiné změny.

  - nároky na údržbu a nákladnost oprav, plán údržby/oprav:
    Provozní zajištění bude v kompetenci žadatele Fakultní nemocnice Brno. Odborné zabezpečení projektu budou zajišťovat pracovníci žadatele ve spolupráci s vysoutěženým poskytovatelem technické podpory.

- **Finanční**
  - popis zajištění financování provozu projektu a jeho udržitelnosti včetně nutné obnovy majetku;
    Vlastníkem výstupů projektu je Ministerstvo zdravotnictví ČR, Fakultní nemocnice Brno, má k majetku právo hospodaření se svěřeným majetkem. Financování provozu projektu bude zabezpečeno z provozního rozpočtu žadatele. Obnova majetku v době udržitelnosti není předpokládána. Jedná se o výstupy – pořízení majetku – HW, a jeho implementace s životností přesahující dobu udržitelnosti.
    IT podpora poskytnutá v době udržitelnosti bude financována z provozního rozpočtu žadatele.

  - pokud se jedná o projekt s celkovými způsobilými výdaji alespoň 100 mil. Kč, žadatel uvede u všech případných příjemců plnění za přímé využití infrastruktury pořízené z IROP (příjemcem plnění v tomto smyslu nemusí být nutně osoba příjemce dotace, může se jednat např. o provozovatele projektu), která jsou zatížená DPH, zda mají tyto subjekty nárok na odpočet DPH na vstupu:
    Nejedná se o projekt s celkovými způsobilými výdaji alespoň 100 mil. Kč – nerelevantní.

- **Administrativní**
  - zajištění administrativní kapacity – počet a kvalifikace lidí, kteří budou řídit projekt v době udržitelnosti;

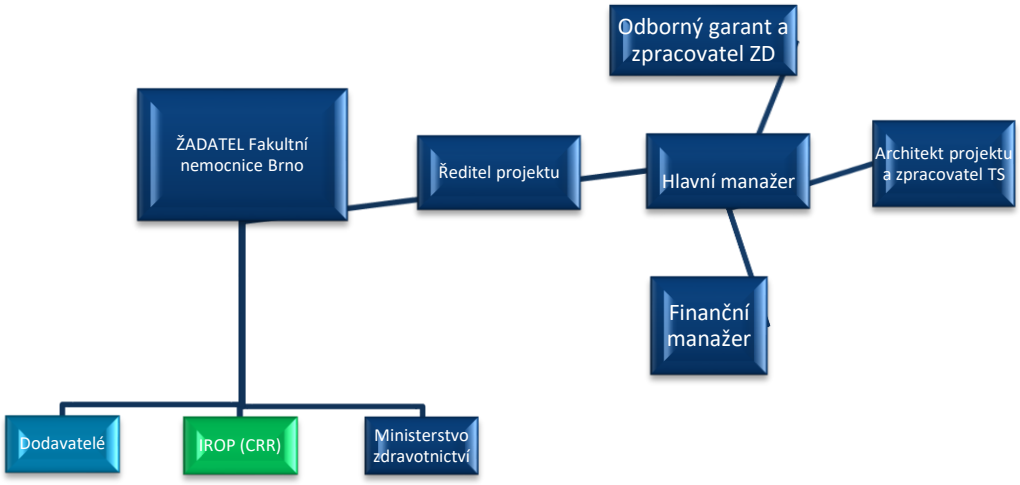
Zodpovědnou osobou v provozní fázi je **Ředitel projektu** (Ing. Peter Mešťaník, náměstek pro informatiku), který je přímo podřízený žadateli a je nadřízený všem ostatním členům týmu. Je zodpovědný za realizaci a úspěch projektu vůči žadateli i zřizovateli. Vedoucí realizačního týmu bude řídit veškerou práci v týmu. Mezi jeho hlavní kompetence bude patřit řízení pracovníků zapojených do udržitelnosti projektu, řízení a monitorování procesů, bude tento projekt zastupovat navenek, zlepšovat komunikaci v týmu a také tento tým motivovat.

Hlavní manažer (Michal Plesar, vedoucí Oddělení pro řízení projektů) je přímo podřízený Řediteli projektu, bude připravovat setkání týmu a vést o něm zápisy, udržovat projektovou dokumentaci, monitorovat provoz projektu. Bude zajišťovat udržitelnost projektu v souladu s podmínkami stanovenými poskytovatelem dotace. Spolupracuje s řídícím orgánem. Účastní se kontrol ze strany řídícího orgánu či vnějších nezávislých kontrol, vykonává kontrolu nad zpracováním Monitorovací zprávy o udržitelnosti

Odborný garant a zpracovatel ZD (Robert Kotzian, Manažer kybernetické bezpečnosti) úzce spolupracuje s Hlavním manažerem projektu za zajištění udržitelnosti technických systémů kybernetické bezpečnosti.

Architekt projektu a zpracovatel TS (Robert Schindler, architekt kybernetické bezpečnosti) bude zajišťovat provoz projektu v souladu s podmínkami pro kybernetickou bezpečnost.

Finanční manažer (Ing. Robert Czékus, MHA, ekonomický náměstek) projektu nese odpovědnost za ekonomické ukazatele, za bezproblémové účetnictví. Mezi další činnosti bude patřit příprava podkladů pro Zprávy o udržitelnosti.



Obrázek č. 2 Organizační struktura projektu (Zdroj: vlastní zpracování)

- popis plnění organizačních opatření – rozsah, personální zajištění.
  V době udržitelnosti bude veškeré úkony spojené s projektem řešit výše uvedený projektový tým, v rámci některých činností může být doplněn o externí odborníky.
  Bude probíhat pravidelný monitoring vůči poskytovateli dotace. Projektový tým bude zajišťovat v pravidelných ročních intervalech předkládání Monitorovacích zpráv o udržitelnosti, jejichž obsahem bude informování o průběhu provozu v době udržitelnosti, plnění cíle projektu a zajištění udržení výstupů projektu.
  Vedení odděleného účetnictví projektu bude zajišťováno interním pracovníkem.

10. VEŘEJNÁ PODPORA

Žadatel o podporu je poskytovatelem služeb obecného hospodářského zájmu dle Rozhodnutí 2012/21/EU.