# 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** | |
| **Členové zpracovatelského týmu, jejich role a kontakty** | |
| **Datum vypracování** | 8/2022 |

## 2. ZÁKLADNÍ INFORMACE O ŽADATELI

| | |
|---|---|
| **Obchodní jméno, sídlo, IČO a DIČ žadatele** | |
| **Jméno, příjmení a kontakt na statutárního zástupce** | , |
| **Jméno, příjmení a kontakt na kontaktní osobu pro projekt** | |
| **Nárok na odpočet DPH na vstupu ve vztahu ke způsobilým výdajům projektu** (Ano x 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<br>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.<br>Cizinci<br>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.<br>Bude také zabezpečena dostupnost zdravotních služeb pro cizince, a to prostřednictvím ochrany informačního systému nemocnice před kybernetickými útoky.<br><br>~~Zaměstnanci ve veřejné zprávě~~<br>~~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.~~<br><br>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.<br><br>~~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.<br>- 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.<br>- 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. 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