Pardubický kraj
Komenského náměstí 125, Pardubice 532 11

č. j. KUPA-13235/2024-1

ZADÁVACÍ DOKUMENTACE

(dále též jako „ZD“)

Veřejný zadavatel
Pardubický kraj
se sídlem Komenského náměstí 125, 532 11 Pardubice
IČO: 708 92 822

vyhlašuje nadlimitní veřejnou zakázku na dodávky
zadávanou v otevřeném řízení dle zákona č. 134/2016 Sb.,
o zadávání veřejných zakázek, v platném znění (dále jen „ZZVZ“)

„Kybernetická bezpečnost poskytovatelů ZS následné péče Pardubického kraje“

1. IDENTIFIKAČNÍ ÚDAJE ZADAVATELE

Název: Pardubický kraj
Právní forma: Veřejnoprávní korporace
Sídlo: Komenského náměstí 125, 532 11 Pardubice
IČO: 708 92 822
DIČ: CZ70892822
Zastoupen: JUDr. Martinem Netolickým, Ph.D., hejtmanem Pardubického kraje
Kontaktní osoba: Mgr. Pavel Menšl, oddělení veřejných zakázek
Tel: +420 466 026 282, +420 605 551 501
E-mail: pavel.mensl@pardubickykraj.cz
Systémové číslo veřejné zakázky na profilu: P24V00000255
Profil zadavatele: https://zakazky.pardubickykraj.cz/profile_display_2.html
Místo přístupu k zadávací dokumentaci: https://zakazky.pardubickykraj.cz/vz00004921

2. PŘEDMĚT VEŘEJNÉ ZAKÁZKY

Předmětem plnění veřejné zakázky je komplexní dodávka a implementace technologií, dodávky SW, HW a infrastruktury pro realizaci technických bezpečnostních opatření dle § 5 odst. 3) zákona č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB) pro zabezpečení NIS provozovaných poskytovateli zdravotních služeb následné péče zřizovaných Pardubickým krajem v rámci výkonu veřejné správy v oblasti poskytování zdravotní péče, kterou Pardubický kraj vykonává na území Pardubického kraje. Součástí plnění VZ jsou dále servisní služby po dobu 5 let.

Podrobnější informace jsou obsaženy v technické specifikaci (příloha č. 2 ZD), popisu servisních služeb (příloha č. 3 ZD) a v návrhu smlouvy (příloha č. 6 ZD).

Klasifikace předmětu veřejné zakázky (CPV):

Název	CPV
Balíky programů a informační systémy	**48000000-8**
Síťová zařízení	32420000-3
Síťová infrastruktura	32424000-1
Informační systémy a servery	48800000-6
Implementace programového vybavení	72263000-6
Podpora programového vybavení	72261000-2
Údržba programového vybavení pro informační technologie	72267100-0

Veřejná zakázka je realizována v rámci projektu „ Kybernetická bezpečnost poskytovatelů zdravotních služeb následné péče Pardubického kraje“, reg. č. CZ.06.01.01/00/22_003/0000043 financovaného prostřednictvím Integrovaného regionálního operačního programu 2021-2027 (dále jen ,,IROP“).

3. PŘEDPOKLÁDÁNA HODNOTA VEŘEJNÉ ZAKÁZKY

Předpokládaná hodnota veřejné zakázky je 73 050 000,00 Kč bez DPH.

4. DOBA A MÍSTO PLNĚNÍ VEŘEJNÉ ZAKÁZKY

Předpokládaný termín plnění: dodávka do 280 dnů od účinnosti smlouvy o dílo, poskytování následných servisních služeb na dobu určitou 5 let), blíže viz návrh smlouvy (příloha č. 6 ZD)

Místo plnění veřejné zakázky: Realizace předmětu plnění bude probíhat v následujících místech plnění:

Místo	Adresa	Předmět realizace
Léčebna dlouhodobě nemocných Rybitví	Činžovních domů 140 Rybitví PSČ: 533 54	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Dodávky bezpečnostních technologií a související služby pro zabezpečení IS.
Vysokomýtská nemocnice	Hradecká 167 Vysoké Mýto PSČ: 566 23	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Dodávky bezpečnostních technologií a související služby pro zabezpečení IS.
	Žižkova 271 Vysoké Mýto PSČ: 566 23	Záložní datové centrum, umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Dodávky bezpečnostních technologií a související služby pro zabezpečení IS.
Nemocnice následné péče Moravská Třebová	Svitavská 25 Moravská Třebová PSČ: 571 16	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Dodávky bezpečnostních technologií a související služby pro zabezpečení IS.
Odborný léčebný ústav Jevíčko	Jevíčko 508 PSČ: 569 43	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Dodávky bezpečnostních technologií a související služby pro zabezpečení IS.
Albertinum, odborný léčebný ústav, Žamberk	Za Kopečkem 353 Žamberk PSČ: 564 21	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Dodávky bezpečnostních technologií a související služby pro zabezpečení IS.
Rehabilitační ústav Brandýs nad Orlicí	Lázeňská 58 Brandýs nad Orlicí, PSČ: 561 12	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Dodávky bezpečnostních technologií a související služby pro zabezpečení IS.
Nemocnice Pardubického kraje, a.s.	Kyjevská 44, Pardubice	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Dodávky bezpečnostních technologií a související služby pro zabezpečení IS.

5. POŽADAVKY NA KVALIFIKACI DODAVATELŮ

Veškeré doklady prokazující splnění kvalifikace postačí v nabídce předložit v prosté kopii. Dodavatel může dle § 86 odst. 2 ZZVZ nahradit předložení kvalifikačních dokladů čestným prohlášením nebo jednotným evropským osvědčením pro veřejné zakázky dle § 87 ZZVZ. Zadavatel nabízí vzor čestného prohlášení uvedený v příloze č. 1 této ZD "formulář nabídky".

Doklady prokazující základní způsobilost a výpis z obchodního rejstříku nebo jiné obdobné evidence musí prokazovat splnění požadované způsobilosti nejpozději v době 3 měsíců před dnem zahájení zadávacího řízení.

5.1. Základní způsobilost

Dodavatel prokazuje základní způsobilost dle **§ 74 odst. 1 písm. a) až e) ZZVZ** způsobem dle **§ 75 odst. 1 ZZVZ**.

Dodavatel tak předloží:

- výpis z evidence Rejstříku trestů ve vztahu k § 74 odst. 1 písm. a)
- potvrzení příslušného finančního úřadu ve vztahu k § 74 odst. 1 písm. b)
- čestné prohlášení ve vztahu ke spotřební dani ve vztahu k § 74 odst. 1 písm. b)
- čestné prohlášení ve vztahu k § 74 odst. 1 písm. c)
- potvrzení okresní správy sociálního zabezpečení ve vztahu k § 74 odst. 1 písm. d)
- výpis z obchodního rejstříku nebo čestné prohlášení ve vztahu k § 74 odst. 1 písm. e)

5.2. Profesní způsobilost

Dodavatel prokazuje profesní způsobilost dle § 77 odst. 1 ZZVZ. Dodavatel tak předloží výpis z obchodního rejstříku nebo jiné obdobné evidence, pokud jiný právní předpis zápis do takové evidence vyžaduje.

5.3. Technická kvalifikace

5.3.1. Seznam významných dodávek

Rozsah a způsob prokázání požadovaných informací a dokladů:
K prokázání kritérií technické kvalifikace podle **§ 79 odst. 2 písm. b) ZZVZ** dodavatel doloží **seznam významných dodávek / služeb** (referencí) poskytnutých za posledních 5 let před zahájením tohoto zadávacího řízení. Dodavatel předloží formou čestného prohlášení seznam významných služeb s uvedením jejich stručného popisu, ceny, termínu realizace a identifikace objednatele.

Minimální úroveň:
Dodavatel prokáže toto kvalifikační kritérium, pokud v posledních 5 letech ode dne zahájení zadávacího řízení realizoval (tzn. zcela dokončil nebo dokončil její poměrnou část splňující dále uvedený finanční limit) alespoň:

a) 2 významné dodávky informačních systémů ve zdravotnictví (nemocniční systémy a technologie ve smyslu této zakázky) obsahující min. jednu z následujících technologií: nástroje pro sběr a vyhodnocování logů, nástroje pro sběr, monitorování a vyhodnocování událostí v rámci komunikačních sítí, nástroje pro ochranu síťového perimetru, nástroje pro ochranu před škodlivým kódem. Z toho alespoň 1 v hodnotě minimálně 10 milionů Kč bez DPH, zbývající v hodnotě minimálně 5 milionů Kč bez DPH za každou jednotlivou významnou zakázku.

b) 2 významné služby na zajišťování kontinuální technické nebo servisní podpory informačních systémů ve zdravotnictví (nemocniční systémy a technologie ve smyslu této zakázky) obsahujícího min. poskytování servisních služeb pro min. jednu z následujících technologií: nástroje pro sběr a vyhodnocování logů, nástroje pro sběr, monitorování a vyhodnocování událostí v rámci komunikačních sítí, nástroje pro ochranu síťového perimetru, nástroje pro ochranu před škodlivým kódem kde je součástí servisu i indikace a předcházení možných problémů v rámci servisované bezpečnostní infrastruktury po dobu souvislých minimálně 24 měsíců s odměnou min. 300.000 Kč bez DPH za jeden rok v rámci každé takové služby.

Zadavatel upřesňuje, že není vyloučeno, aby byly shora uvedené požadavky dle bodu a) a b) splněny stejnou referenční zakázkou.

Zadavatel dále doplňuje, že dodané nebo podporované informační systémy pro účely prokázání shora uvedených kvalifikačních požadavků musely být provozovány a využívány pro práci svými uživateli v nepřetržitém provozu, tj. 365 dní v roce, 7 dní v týdnu, 24 hodin denně.

5.3.2. Seznam členů realizačního týmu

Rozsah a způsob prokázání požadovaných informací a dokladů

K prokázání kritérií technické kvalifikace dodavatel doloží seznam osob tvořících realizační tým dodavatele, které se budou přímo podílet na poskytování služeb, a osvědčení o jejich odborné kvalifikaci dle ust. § 79 odst. 2 písm. c), d) ZZVZ (dále také „Seznam členů“). Dodavatel prokazuje tuto část kvalifikace předložením profesních životopisů jednotlivých členů realizačního týmu. Z dodavatelem předložených podkladů musí jednoznačně vyplývat splnění všech podmínek a požadavků na členy realizačního týmu uvedené dále (k prokázání relevantních zkušeností musí být v životopisech uvedeny konkrétní projekty, kterých se tyto osoby účastnily a na jaké pozici, včetně uvedení subjektů, pro které byly projekty realizovány, přesného vymezení předmětu projektu, doby realizace a kontaktních údajů na objednatele).

Minimální úroveň:

Dodavatel předloží seznam členů realizačního týmu, kteří se budou podílet na plnění veřejné zakázky bez ohledu na to, zda jde o zaměstnance dodavatele nebo osoby v jiném vztahu k dodavateli. Realizační tým tvoří minimálně **6** osob, které musí splňovat požadavky na jednotlivé role definované níže:

a) Vedoucí realizačního týmu – 1 osoba

- Má alespoň 5 let praxe v oboru informačních technologií.
- Disponuje jazykovou znalostí českého jazyka (případně slovenského) na úrovni pracovní komunikace.
- Realizoval minimálně 2 referenční zakázky v posledních 5 letech před zahájením zadávacího řízení, jejichž předmětem byla dodávka a implementace informačních systémů anebo bezpečnostních technologií do zdravotnictví. Alespoň jedna zakázka byla v hodnotě minimálně 10 000 000 Kč bez DPH, ostatní zakázky byly v hodnotě minimálně 5 000 000 Kč bez DPH pro každou zakázku zvlášť.
- disponuje platnou certifikací v oblasti projektového řízení PRINCE2, PMP, IPMA nebo ekvivalentu uvedených certifikátů vystavených od jiných oprávněných subjektů.

b) Technický specialista – zabezpečení NIS – 3 osoby

- Má alespoň 5 let praxe v oboru informačních technologií.
- Disponuje jazykovou znalostí českého jazyka (případně slovenského) na úrovni pracovní komunikace.
- Realizoval minimálně 1 referenční zakázku za posledních 5 let před zahájením zadávacího řízení, jejichž předmětem byla dodávka a implementace úprav nemocničního informačního systému (dle technické specifikace) pro napojení na bezpečnostní technologie (sběr a analýza logů, napojení na MS AD nebo IdM) v hodnotě minimálně 1 000 000 Kč bez DPH pro každou zakázku zvlášť.
- Kvalifikace musí být splněna min. jednou osobou pro každý ze zabezpečovaných IS (FONS Akord, FONS Enterprise, LBIS/4G).

c) Technický specialista – analýza bezpečnostních logů – 1 osoba

- Musí mít alespoň 5 let praxe v oboru informačních technologií.
- Disponuje jazykovou znalostí českého jazyka (případně slovenského) na úrovni pracovní komunikace.
- Realizoval minimálně 1 referenční zakázku za posledních 5 let před zahájením zadávacího řízení, jejímž předmětem bylo nasazení sběru a analýzy logů informačních systémů a technologií ve zdravotnictví, který v sobě integruje jak analýzu logů IS, tak okolí systému (komunikační, bezpečnostní a serverová infrastruktura) a je aktuálně provozován v hodnotě minimálně 2 000 000 Kč bez DPH.

d) Specialista řešení kybernetických bezpečnostních incidentů – 1 osoba

- Musí mít alespoň 5 let praxe v oboru informačních technologií.
- Disponuje jazykovou znalostí českého jazyka (případně slovenského) na úrovni pracovní komunikace.
- Splňuje kvalifikaci dle Přílohy č. 6 k vyhlášce č. 82/2018 Sb., popis kvalifikačních požadavků pro bezpečnostní role uvedené v § 6 a 7, Tab. 2: Manažer kybernetické bezpečnosti nebo Tab. 4: Auditor kybernetické bezpečnosti.
- Realizoval minimálně 1 referenční zakázku za posledních 5 let před zahájením zadávacího řízení, jejímž předmětem byl bezpečnostní audit v prostředí organizace regulované ZKB.
- Realizoval minimálně 1 referenční zakázku za posledních 5 let před zahájením zadávacího řízení, jejímž předmětem bylo provedení penetračního testu infrastrukturního nebo aplikačního prostředí v prostředí organizace regulované ZKB.
- Má znalost architektury technických bezpečnostních opatření, k prokázání tohoto požadavku dodavatel předloží certifikát CompTIA Security+ nebo CISSP nebo obdobný certifikát specialisty dle Vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti.

- Má certifikaci CompTIA Security Analytics Expert (CSAE) – Expert-level, k prokázání tohoto požadavku dodavatel předloží certifikát, tato certifikace je udělena těm, kteří mají kombinaci certifikátů Security + / CySA + / CASP nebo obdobný certifikát specialisty.

5.4. Prokázání kvalifikace prostřednictvím jiných osob (§ 83)

Dodavatel může prokázat určitou část technické kvalifikace nebo profesní způsobilosti s výjimkou kritéria podle § 77 odst. 1 ZZVZ prostřednictvím jiných osob. Dodavatel je v takovém případě povinen zadavateli předložit:

a) doklady prokazující splnění profesní způsobilosti podle § 77 odst. 1 ZZVZ jinou osobou,
b) doklady prokazující splnění chybějící části kvalifikace prostřednictvím jiné osoby,
c) doklady o splnění základní způsobilosti podle § 74 ZZVZ jinou osobou,
d) smlouvu nebo jinou osobou o podepsané potvrzení o její existenci, jejímž obsahem je písemný závazek jiné osoby k poskytnutí plnění určeného k plnění veřejné zakázky nebo k poskytnutí věcí nebo práv, s nimiž bude dodavatel oprávněn disponovat při plnění veřejné zakázky, a to alespoň v rozsahu, v jakém jiná osoba prokázala kvalifikaci za dodavatele.

5.5. Předkládání dokladů

Pokud není dodavatel z důvodů, které mu nelze přičítat, schopen předložit požadovaný doklad, je oprávněn předložit jiný rovnocenný doklad.

6. PROHLÁŠENÍ DLE Z. Č. 159/2006 SB., O STŘETU ZÁJMŮ DLE NAŘÍZENÍ RADY (EU) 2022/576

Dodavatel v nabídce předloží čestné prohlášení (příloha “formulář nabídky“), že

- není obchodní společností, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) zák. č. 159/2006 Sb., o střetu zájmů, v platném znění nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti a
- že neprokazuje svou kvalifikaci prostřednictvím osoby uvedené v předchozí odrážce.
- že není dodavatelem, který je:
  a) ruským státním příslušníkem, fyzická či právnická osoba nebo subjekt či orgán se sídlem v Rusku,

  b) právnickou osobou, subjektem nebo orgánem, který je z více než 50 % přímo či nepřímo vlastněn některým ze subjektů uvedených v písmeni a) výše, nebo

  c) fyzickou nebo právnickou osobou, subjektem nebo orgánem, které jednají jménem nebo na pokyn některého ze subjektů uvedených v písmeni a) nebo b) výše, včetně subdodavatelů, dodavatelů nebo subjektů, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, pokud představují více než 10 % hodnoty zakázky, nebo společně s nimi.

7. OBCHODNÍ A PLATEBNÍ PODMÍNKY

7.1. Dodavatel je povinen respektovat obchodní a platební podmínky uvedené v návrhu smlouvy, který tvoří přílohu č. 6 této ZD.

7.2. Zadavatel stanoví, že součástí nabídky dodavatele nebude podepsaný návrh smlouvy, ale akceptace smluvních a obchodních podmínek. Zadavatel nabízí ke splnění tohoto požadavku vzorové čestné prohlášení (viz příloha “formulář nabídky“).

S vybraným dodavatelem pak bude uzavřena smlouva v souladu s návrhem smlouvy uvedeným v této ZD a akceptací dodavatele, a to zásadně v elektronické podobě.

8. TECHNICKÉ PODMÍNKY, PROHLÍDKA MÍSTA PLNĚNÍ

Technické podmínky vymezující předmět veřejné zakázky jsou uvedeny v přílohách této zadávací dokumentace, zejména v příloze č. 2 (Technická specifikace), 3 (Servisní služby) a 6 (Návrh smlouvy).

9. ROVNÉ PODMÍNKY HOSPODÁŘSKÉ SOUTĚŽE

V rámci VZ a jejího předmětu identifikoval zadavatel následující potenciálně unikátní dodavatele stávajících technologií na všech lokalitách, kde by mohlo dojít k marginálnímu omezení hospodářské soutěže z důvodu nutných zásahů do nemocničního informačního systému (NIS):

Identifikace společnosti	Oblast unikátnosti	Zdravotnické zařízení	Popis potenciální unikátnosti
STAPRO s. r. o. IČO: 13583531 Sídlo: Pernštýnské náměstí 51, Pardubice-Staré Město, 530 02 Pardubice	Nemocniční informační systém	Léčebna dlouhodobě nemocných Rybitví	NIS pro ZZ PAK dodala a servisní služby poskytuje uvedená společnost. Neautorizovaný zásah do NIS by byl zásahem do dodávky uvedeného dodavatele, přičemž by mohlo dojít k porušení podmínek uzavřených smluv. Autorizované úpravy systému NIS je schopna provést jen uvedená společnost, případně její subdodavatelé.
		Odborný léčebný ústav Jevíčko	
		Albertinum, odborný léčebný ústav Žamberk	
		Nemocnice následné péče Moravská Třebová	
		Vysokomýtská nemocnice	
LAURYN s.r.o. IČO: 60113685 Sídlo: Pardubice - Staré Čívice, Přeloučská 255, PSČ 53006	Nemocniční informační systém	Rehabilitační ústav Brandýs nad Orlicí	

Na základě uvedených skutečností zadavatel zajistil před zahájením zadávacího řízení rovný přístup pro dodavatele VZ pro případ, že jejich technické řešení bude navázáno na stávající poskytovatele NIS prostřednictvím proklamací společností STAPRO s.r.o. i LAURYN s.r.o., viz příloha č. 8 ZD (a to vedle stávajících platných servisních smluv).

10. POŽADAVKY NA ZPŮSOB ZPRACOVÁNÍ NABÍDKOVÉ CENY

10.1. Nabídkovou cenu dodavatel uvede v podbarveném sloupci v položkovém rozpočtu (příloha č. 4 ZD). Množstevní ceny a ceny vč. DPH jsou generovány rozpočtem automaticky za použití matematického vzorce. Cena včetně DPH je cenou nejvýše přípustnou a zahrnuje v souladu s požadovanou specifikací dodávky veškeré náklady dodavatele vzniklé v souvislosti s realizací předmětu veřejné zakázky. Cena může být měněna pouze v souvislosti se změnou daňových předpisů majících prokazatelný vliv na uvedenou cenu. Ceny musí být uvedeny bez DPH, částka DPH a včetně DPH.

9.2. Nebude-li součástí nabídky dodavatele údaj o nabídkové ceně (zásadně vyplněný položkový rozpočet), bude dodavatel vyloučen z účasti na zadávacím řízení.

11. POŽADAVKY NA ZPRACOVÁNÍ A ČLENĚNÍ NABÍDKY

10.1 Nabídka:

- bude předložena v elektronické podobě pomocí elektronického nástroje E-ZAK dostupného na https://zakazky.pardubickykraj.cz/,
- bude zpracována v českém jazyce. Zadavatel připouští použití rovněž anglického jazyka v částech nabídky, kde bude účastník zadávacího řízení používat odborné termíny a názvosloví týkající se technické specifikace a popisu nabízeného předmětu plnění,
- bude obsahovat akceptaci smluvních a obchodních podmínek (viz formulář nabídky),

- bude obsahovat čestné prohlášení o opatřeních ve vztahu k mezinárodním sankcím (viz příloha č. 7 ZD),
- bude obsahovat položkový rozpočet (viz příloha č. 4)
- bude obsahovat vyplněnou hodnotící tabulku (viz příloha č. 5 ZD),
- bude obsahovat popis dodavatelem navrhované součinnosti objednatele (viz formulář nabídky),
- bude obsahovat doklady, jimiž dodavatel prokazuje splnění podmínek účasti (kvalifikace, prohlášení ke střetu zájmů).

10.2 Zadavatel doporučuje dodavatelům, aby zpracovali nabídku v následujícím členění:

- formulář nabídky (viz příloha č. 1 ZD),
- doklady o splnění kvalifikace – kopie dokladů nebo čestné prohlášení dle přílohy „formulář nabídky“ nebo jednotné evropské osvědčení pro veřejné zakázky,
- čestné prohlášení o opatřeních ve vztahu k mezinárodním sankcím (viz příloha č. 7 ZD),
- položkový rozpočet (viz příloha č. 4 ZD)
- hodnotící tabulka (viz příloha č. 5 ZD)

12. LHŮTA, FORMA A ZPŮSOB PODÁNÍ NABÍDEK, KOMUNIKACE

11.1. Lhůta pro podání nabídky

Nabídku doručte nejpozději **do 2. 9. 2024 do 10:00 hod.**

11.2. Forma a způsob podání nabídek
Zadavatel dle ust. § 103 odst. 1 písm. c) a § 107 odst. 1 ZZVZ stanovil pouze elektronickou formu nabídek. Nabídky se podávají prostřednictvím elektronického nástroje E-ZAK (https://zakazky.pardubickykraj.cz/) vložením její elektronické podoby přes odkaz „poslat nabídku“ na kartě této veřejné zakázky.

11.3. Komunikace
Veškeré úkony v zadávacím řízení a veškerá komunikace probíhají elektronicky, zásadně prostřednictvím elektronického nástroje E-ZAK, datové schránky a e-mailu. Dodavatel je povinen provést **registraci v elektronickém nástroji**.
Podrobné informace o ovládání systému naleznete v uživatelské příručce a manuálu appletu elektronického podpisu.

V případě jakýchkoli otázek týkajících se technického nastavení kontaktujte, prosím, provozovatele elektronického nástroje E-ZAK na e-mailu: podpora@ezak.cz; podpora@fen.cz nebo tel. čísle +420 515 917 947; +420 538 702 719.

11.4. Vzhledem k elektronické podobě nabídek neprobíhá veřejné otevírání nabídek.

13. ZADÁVACÍ LHŮTA

Zadavatel stanovuje zadávací lhůtu v délce 3 měsíců od konce lhůty pro podání nabídek. Účastník zadávacího řízení nesmí po dobu běhu zadávací lhůty ze zadávacího řízení odstoupit.

14. PRAVIDLA PRO HODNOCENÍ NABÍDEK

Zadavatel bude nabídky hodnotit dle jejich ekonomické výhodnosti. Ekonomická výhodnost bude hodnocena na základě nejvýhodnějšího poměru nabídkové ceny a kvality. Přehled kritérií hodnocení včetně jejich váhy je uveden v následující tabulce:

Dílčí kritéria hodnocení		váha
1.	Nabídková cena	70%
2.	Celková kvalita nabídky	30%

Dodavatel vyplní údaje pro hodnocení do položkového rozpočtu (příloha č. 4 ZD) a hodnotící tabulky, která je přílohou č. 5 této ZD, a doloží níže požadované doklady.

- **Kritérium č. 1 – „Nabídková cena“**

Hodnocena bude výše celkové nabídkové ceny v Kč včetně DPH uvedená dodavatelem v položkovém rozpočtu. Za nejvýhodnější bude považována nabídka s nejnižší nabídkovou cenou. Bodová hodnota dílčího kritéria jednotlivých nabídek vznikne násobkem 100, poměru hodnoty nejvýhodnější nabídky k hodnocené nabídce a váhy daného kritéria:

Počet bodů = 100 x nejvýhodnější nabídka / hodnocená nabídka x 70 %

- **Kritérium č. 2 – „Celková kvalita nabídky“**

V rámci hodnocení celkové kvality nabídky budou hodnoceny zkušenosti členů realizačního týmu, které jsou nad rámec minimálních kvalifikačních požadavků stanovených v bodě 5.3.2. Dodavatel získá bodové ohodnocení v případě splnění níže uvedených podmínek:

Způsob hodnocení	
1. Kvalifikační minimum u každého člena realizačního týmu = 1 referenční zakázka dle podmínek stanovených v bodě 5.3.2. Zakázku, kterou dodavatel prokazuje kvalifikaci, nelze zohlednit v rámci hodnocení. Hodnoceny budou pouze zakázky nad rámec zakázek kvalifikačních. 2. Za každou hodnocenou referenční zakázku získá dodavatel bodové ohodnocení, maximálně však bude hodnoceno 5 referenčních zakázek za každého jednotlivého člena realizačního týmu. 3. Způsob udělení bodů: a. Za zakázku v oblasti zdravotnictví dodavatel získá 2 body b. Za zakázku mimo oblast zdravotnictví dodavatel získá 1 bod c. Maximální možný počet bodů v rámci tohoto hodnotícího kritéria: 3 členové * 10 bodů = 30 bodů	
Vedoucí realizačního týmu	Max. 5 zakázek dle definice v bodě 5.3.2. a) ZD v min. realizovaném finančním objemu 2 000 000 Kč bez DPH za každou zakázku. Pokud bude zakázka v oblasti zdravotnictví, dodavatel získá 2 body, za zakázku mimo oblast zdravotnictví bude přidělen 1 bod.
Technický specialista – analýza bezpečnostních logů	Max. 5 zakázek dle bodu 5.3.2. c) ZD v min. realizovaném finančním objemu 500 000 Kč bez DPH za každou zakázku. Pokud bude zakázka v oblasti zdravotnictví, dodavatel získá 2 body, za zakázku mimo oblast zdravotnictví bude přidělen 1 bod.
Specialista řešení kybernetických bezpečnostních incidentů	Max. 5 zakázek dle bodu 5.3.2. d) ZD v min. realizovaném finančním objemu 500 000 Kč bez DPH za každou zakázku. Pokud bude zakázka v oblasti zdravotnictví, dodavatel získá 2 body, za zakázku mimo oblast zdravotnictví bude přidělen 1 bod.

Splnění podmínek kladených na referenční zakázky, které jsou předmětem hodnocení, dodavatel prokáže doložením čestného prohlášení s uvedením názvu zakázky, termínu realizace zakázky, stručného popisu obsahu plnění zakázky, ceny, názvu objednatele, kontaktní osoby objednatele, která je oprávněna sdělovat informace potřebné k ověření splnění výše uvedených podmínek. Zadavatel pro tyto účely vytvořil formulář hodnotící tabulky, která tvoří přílohu č. 5 zadávací dokumentace.

Výsledná bodová hodnota dílčího kritéria (celková kvalita nabídky) jednotlivých nabídek vznikne násobkem 100 poměru součtu bodů hodnocené nabídky k součtu bodů nejvýhodnější nabídky a váhy daného kritéria:

Počet bodů = 100 x součet bodů hodnocené nabídky / součet bodů nejvýhodnější nabídky x 30 %

- **Celkové hodnocení**

Na základě součtu výsledných bodových hodnot kritérií u jednotlivých nabídek bude stanoveno pořadí úspěšnosti nabídek. Jako nejúspěšnější bude stanovena nabídka, která v součtu za obě dílčí kritéria dosáhla nejvyšší hodnoty. Na základě celkového bodového ohodnocení stanoví hodnotící komise výsledné pořadí nabídek. Bodové ohodnocení bude zadavatel ve všech případech zaokrouhlovat na 2 desetinná místa. V případě rovnosti bodových hodnot dvou či více nabídek rozhoduje o celkovém pořadí nabídek pořadí v kritériu č. 1 „Nabídkové ceně“. Pokud by došlo ke shodě i v nabídkových cenách, rozhoduje o nejvýhodnější nabídce losování, které

proběhne za přítomnosti notáře v sídle zadavatele a za účasti účastníků, jejichž nabídkové ceny byly shodné. Pravidla pro losování sdělí zadavatel dotčeným osobám v předstihu nejméně 5 pracovních dní.

Zadavatel neprovede hodnocení nabídek, pokud by měl hodnotit nabídku pouze jednoho dodavatele.

Dodavatel musí v nabídce doložit údaje rozhodné pro hodnocení (zásadně vyplněný položkový rozpočet a hodnotící tabulka). Jejich pozdější doplňování je dle § 46 ZZVZ nepřípustné. Zadavatel upozorňuje dodavatele, že není možné v průběhu posuzování a hodnocení nabídek měnit údaje a doklady určené pro hodnocení nabídek. Přípustné je pouze jejich objasňování.

15. DALŠÍ PODMÍNKY

15.1. Informace o skutečném majiteli vybraného dodavatele budou zadavatelem zjišťovány postupem dle ust. § 122 odst. 4 nebo 5 ZZVZ.

15.2. Zadavatel si v souladu s § 104 písm. e/ ZZVZ vyhrazuje povinnost vybraného dodavatele předložit před uzavřením smlouvy v rámci jeho součinnosti následující dokumenty:

- pojistnou smlouvu s pojistným plněním ve výši 50 mil. Kč, viz čl. VII návrhu smlouvy,
- osvědčení o tom, že vybraný dodavatel je certifikovaným nebo autorizovaným partnerem výrobce pro nabízené technologie, min. pro nástroje pro sběr a vyhodnocování logů, nástroje pro sběr, monitorování a vyhodnocování událostí v rámci komunikačních sítí.

15.3. Zadavatel posoudil zadávací podmínky rovněž z pohledu zásady sociálně odpovědného zadávání, environmentálně odpovědného zadávání a inovací. Vzhledem k povaze a smyslu veřejné zakázky není přiměřený žádný dopad zásady sociálně odpovědného zadávání, environmentálně odpovědného zadávání a inovací na tvorbu zadávacích podmínek, hodnocení a výběr dodavatele.

16. PŘÍLOHY

Nedílnou součástí jsou následující přílohy:

1. Formulář nabídky
2. Technická specifikace
3. Servisní služby
4. Položkový rozpočet
5. Hodnotící tabulka
6. Návrh smlouvy
7. Čestné prohlášení o opatřeních ve vztahu k mezinárodním sankcím
8. Čestná prohlášení NIS

PhDr. Jana Haniková
vedoucí kanceláře ředitele úřadu
pověřená hejtmanem

schváleno usnesením Rady Pardubického kraje dne 1. 7. 2024, č. R/2376/24

Formulář nabídky

1.1. Název veřejné zakázky	**Kybernetická bezpečnost poskytovatelů ZS následné péče Pardubického kraje**
1.2. Identifikační údaje o zadavateli **Název**	Pardubický kraj
Sídlo	Komenského nám. 125, 532 11 Pardubice
IČO	708 92 822
1.3. Druh veřejné zakázky	služby
1.4. Forma zadávacího řízení	nadlimitní zakázka zadávaná v otevřeném řízení
1.5. Systémové číslo profilu	P24V00000255

Zadavatel poskytuje pro potřeby dodavatele formulář nabídky se vzory potřebných prohlášení ke splnění požadavků v zadávací dokumentaci č. j. KUPA-13235/2024-1 na předmětnou veřejnou zakázku.

Formulář nabídky

Název veřejné zakázky	
Kybernetická bezpečnost poskytovatelů ZS následné péče Pardubického kraje	
Identifikační a kontaktní údaje dodavatele	
Obchodní firma	(doplní dodavatel)
IČO	(doplní dodavatel)
Sídlo	(doplní dodavatel)
Číslo účtu	(doplní dodavatel)
Kontaktní osoba	(doplní dodavatel)
E-mail	(doplní dodavatel)
Telefon	(doplní dodavatel)
Osoba oprávněná jednat za dodavatele	
Jméno, příjmení	(doplní dodavatel)
Funkce	(doplní dodavatel)

Čestné prohlášení o splnění podmínek kvalifikace
dle ust. § 86 odst. 2 z. č. 134/2016 Sb., o zadávání veřejných zakázek

Pro účely zadávacího řízení na shora uvedenou veřejnou zakázku prohlašuji, že shora uvedený dodavatel splňuje veškeré podmínky kvalifikace požadované zadavatelem v zadávací dokumentaci čj. KUPA-13235/2024-1, tedy:

1. je způsobilým dle § 74 ZZVZ (kromě jiného nemá v České republice nebo v zemi svého sídla v evidenci daní ve vztahu ke spotřební dani zachycen splatný daňový nedoplatek a že nemá v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění).

2. Splňuje profesní způsobilost dle bodu 5.2. zadávací dokumentace.

3. Splňuje technickou kvalifikaci dle bodu 5.3. zadávací dokumentace.

Seznam významných dodávek dodavatele
dle bodu 5.3.1. zadávací dokumentace

1.	Název a stručný popis předmětu dodávky / služby (včetně popisu technologií a informace o splnění podmínky nepřetržitého provozu)	(doplní dodavatel)
	Termín realizace služby	(doplní dodavatel)
	Identifikace objednatele služby	(doplní dodavatel)
	Kontaktní osoba objednatele vč. kontaktu na ni	(doplní dodavatel)

	Hodnota služby v Kč bez DPH	(doplní dodavatel)
2.	Název a stručný popis předmětu dodávky / služby (včetně popisu technologií a informace o splnění podmínky nepřetržitého provozu)	(doplní dodavatel)
	Termín realizace služby	(doplní dodavatel)
	Identifikace objednatele služby	(doplní dodavatel)
	Kontaktní osoba objednatele vč. kontaktu na ni	(doplní dodavatel)
	Hodnota služby v Kč bez DPH	(doplní dodavatel)
3.	Název a stručný popis předmětu dodávky / služby (včetně popisu technologií a informace o splnění podmínky nepřetržitého provozu)	(doplní dodavatel)
	Termín realizace služby	(doplní dodavatel)
	Identifikace objednatele služby	(doplní dodavatel)
	Kontaktní osoba objednatele vč. kontaktu na ni	(doplní dodavatel)
	Hodnota služby v Kč bez DPH	(doplní dodavatel)
4.	Název a stručný popis předmětu dodávky / služby (včetně popisu technologií a informace o splnění podmínky nepřetržitého provozu)	(doplní dodavatel)
	Termín realizace služby	(doplní dodavatel)
	Identifikace objednatele služby	(doplní dodavatel)
	Kontaktní osoba objednatele vč. kontaktu na ni	(doplní dodavatel)
	Hodnota služby v Kč bez DPH	(doplní dodavatel)

Seznam členů realizačního týmu
dle bodu 5.3.2. zadávací dokumentace

Dodavatel předloží seznam členů realizačního týmu, kteří se budou podílet na plnění veřejné zakázky bez ohledu na to, zda jde o zaměstnance dodavatele nebo osoby v jiném vztahu k dodavateli. Realizační tým tvoří minimálně 6 osob, které musí splňovat požadavky na jednotlivé role definované v bodě 5.3.2. ZD.
Dodavatel prokazuje tuto část kvalifikace předložením profesních životopisů jednotlivých členů realizačního týmu.

a)	**Vedoucí realizačního týmu**
Jméno, příjmení, titul:	(doplní dodavatel)
Zakázka dle bodu 5.3.2. a), kterou dodavatel prokazuje kvalifikaci: (Tuto zakázku dodavatel nemůže uplatnit současně v rámci hodnocení)	(dodavatel doplní název a stručný popis zakázky, termín realizace, realizovaný finanční rozsah v Kč bez DPH, název a kontaktní údaje objednatele zakázky)
b)	**Technický specialista – zabezpečení NIS – FONS Akord**
Jméno, příjmení, titul:	(doplní dodavatel)

Zakázka dle bodu 5.3.2. b), kterou dodavatel prokazuje kvalifikaci: (Tuto zakázku dodavatel nemůže uplatnit současně v rámci hodnocení)	(dodavatel doplní název a stručný popis zakázky, termín realizace, realizovaný finanční rozsah v Kč bez DPH, název a kontaktní údaje objednatele zakázky)
b)	**Technický specialista – zabezpečení NIS – FONS Enterprise**
Jméno, příjmení, titul:	(doplní dodavatel)
Zakázka dle bodu 5.3.2. b), kterou dodavatel prokazuje kvalifikaci: (Tuto zakázku dodavatel nemůže uplatnit současně v rámci hodnocení)	(dodavatel doplní název a stručný popis zakázky, termín realizace, realizovaný finanční rozsah v Kč bez DPH, název a kontaktní údaje objednatele zakázky)
b)	**Technický specialista – zabezpečení NIS – LBIS/4G**
Jméno, příjmení, titul:	(doplní dodavatel)
Zakázka dle bodu 5.3.2. b), kterou dodavatel prokazuje kvalifikaci: (Tuto zakázku dodavatel nemůže uplatnit současně v rámci hodnocení)	(dodavatel doplní název a stručný popis zakázky, termín realizace, realizovaný finanční rozsah v Kč bez DPH, název a kontaktní údaje objednatele zakázky)
c)	**Technický specialista – analýza bezpečnostních logů**
Jméno, příjmení, titul:	(doplní dodavatel)
Zakázka dle bodu 5.3.2. a), kterou dodavatel prokazuje kvalifikaci: (Tuto zakázku dodavatel nemůže uplatnit současně v rámci hodnocení)	(dodavatel doplní název a stručný popis zakázky, termín realizace, realizovaný finanční rozsah v Kč bez DPH, název a kontaktní údaje objednatele zakázky)
d)	**Specialista řešení kybernetických bezpečnostních incidentů**
Jméno, příjmení, titul:	(doplní dodavatel)
Zakázka dle bodu 5.3.2. a), kterou dodavatel prokazuje kvalifikaci: (Tuto zakázku dodavatel nemůže uplatnit současně v rámci hodnocení)	(dodavatel doplní název a stručný popis zakázky, termín realizace, realizovaný finanční rozsah v Kč bez DPH, název a kontaktní údaje objednatele zakázky)

Čestné prohlášení dle z. č. 159/2006 Sb., o střetu zájmů a dle nařízení vlády (EU) 2022/576

Pro účely zadávacího řízení na shora uvedenou veřejnou zakázku prohlašuji, že shora uvedený dodavatel

- není obchodní společností, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) zák. č. 159/2006 Sb., o střetu zájmů, v platném znění nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti a
- že neprokazuje svou kvalifikaci prostřednictvím osoby uvedené v předchozí odrážce.
- že není dodavatelem, který je:

  a) ruským státním příslušníkem, fyzická či právnická osoba nebo subjekt či orgán se sídlem v Rusku,

  b) právnickou osobou, subjektem nebo orgánem, který je z více než 50 % přímo či nepřímo vlastněn některým ze subjektů uvedených v písmeni a) výše, nebo

  c) fyzickou nebo právnickou osobou, subjektem nebo orgánem, které jednají

jménem nebo na pokyn některého ze subjektů uvedených v písmeni a) nebo b) výše, včetně subdodavatelů, dodavatelů nebo subjektů, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, pokud představují více než 10 % hodnoty zakázky, nebo společně s nimi.
Dodavatelem navrhovaná součinnost objednatele
(doplní dodavatel)
Souhlas se smluvními a obchodními podmínkami
Pro účely zadávacího řízení na shora uvedenou veřejnou zakázku prohlašuji, že shora uvedený dodavatel souhlasí se smluvními a obchodními podmínkami, které byly součástí zadávací dokumentace v užším slova smyslu, č. j. KUPA-13235/2024-1, a že v případě, kdy bude vybraným dodavatelem, uzavře smlouvu v souladu s takto stanovenými podmínkami.
V (doplní dodavatel) dne (doplní dodavatel)

Příloha č. 2: Technická specifikace

V této příloze jsou uvedeny výchozí podmínky a požadavky na dodávku v rámci této veřejné zakázky.

OBSAH

VYUŽITÉ ZDROJE

Nejsou

SEZNAM TABULEK

SEZNAM ZKRATEK A POJMŮ

Zkratka/pojem	Význam
365x7x24	Poskytování služeb 365 dní v roce, 7 dnů v týdnu, 24 hodin denně
3E	Principy účelnosti, hospodárnosti a efektivnosti
ADS	Anomálie datové sítě
CERT	Computer Emergency Response Team – Tým pro reakci na kybernetické hrozby - GovSERT.CZ
ČR	Česká republika
ČSN	Česká státní norma
DB	Databáze
DC	Datové centrum
DLP	Data Loss Prevention – technologie pro prevenci ztráty dat
DMZ	Demilitarizované zóna
EDR	Endpoint Detection and Response – Detekce a reakce koncových bodů
EU	Evropská unie
EZD	Elektronická zdravotnická dokumentace
Firewall	Síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení
FlowMon	Nástroje monitorování a bezpečnost počítačových sítí
GDPR	General Data Protection Regulation – Nařízení EU č. 2016/679 o ochraně osobních údajů
GUI	Grafické uživatelské rozhraní
HW	Hardware
IS	Informační systém
LAN	Local Area Network – Místní počítačová síť
LDN	Léčebna dlouhodobě nemocných
LOGManager	Systém pro centralizovanou správu, logmanagement eventů a logů
MS	Microsoft
MS AD	Microsoft Active Directory
NAS	Network Attached Storage – chytrá datová úložiště
NBD	Next Business Day – podpora odstranění problému do dalšího pracovního dne

Zkratka/pojem	Význam
NetFlow	Nástroje monitorování a bezpečnost počítačových sítí
NGFW	Next Generation Firewall - Nástroje pro ochranu síťového perimetru
NIS	Nemocniční informační systém
NNP	Nemocnice následné péče
NPK	Nemocnice Pardubického kraje a.s.
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OS	Operační systém
OWASP	Open Web Application Security Project – Projekt a komunita zabývající se bezpečností webových aplikací
PAK	Pardubický kraj
PNK	Prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018
RDS	Regionální datová síť
SIEM	Security Informativní and Event Management – řešení zabezpečení, které organizacím pomáhá detekovat hrozby, analyzovat je a reagovat na ně dříve, než způsobí škody v provozu firmy
SLA	Úroveň a podmínky poskytování služeb technické a technologické podpory
SOC	Security Operations Center – Bezpečnostní operační centrum
SQL	Strukturovaný dotazovací jazyk pro práci v relačních databázích
SW	Software
UTM	řešení
VZ	Veřejná zakázka
WiFi	Bezdrátová síť
WSTG	Web Security Testing Guide
ZD	Zadávací dokumentace
ZKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
ZS	Zdravotnické služby
ZZ	Zdravotnické zařízení

Tabulka 1: Seznam zkratek a pojmů

1 PŘEDMĚT PLNĚNÍ

Předmětem plnění veřejné zakázky (dílem) je komplexní dodávka a implementace technologií, dodávky SW, HW a infrastruktury pro realizaci technických bezpečnostních opatření dle § 5 odst. 3) zákona č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB) pro zabezpečení NIS provozovaných poskytovateli zdravotních služeb následné péče zřizovaných Pardubickým krajem (žadatel) v rámci výkonu veřejné správy v oblasti poskytování zdravotní péče, kterou Pardubický kraj vykonává na území Pardubického kraje Součástí plnění VZ jsou dále servisní služby po dobu udržitelnosti projektu.

Konkrétně se jedná o zvýšení kybernetické bezpečnosti pro následující IS (dle výzvy ostatní IS):

1. Léčebna dlouhodobě nemocných Rybitví – Nemocniční informační systém – jedná se o primární IS sloužící pro hlavní činnost ZZ (správce), tj. pro poskytování následné zdravotní péče na území Pardubického kraje.
2. Odborný léčebný ústav Jevíčko – Nemocniční informační systém – jedná se o primární IS sloužící pro hlavní činnost ZZ (správce), tj. pro poskytování následné zdravotní péče na území Pardubického kraje.
3. Albertinum, odborný léčebný ústav Žamberk – Nemocniční informační systém – jedná se o primární IS sloužící pro hlavní činnost ZZ (správce), tj. pro poskytování následné zdravotní péče na území Pardubického kraje.
4. Nemocnice následné péče Moravská Třebová – Nemocniční informační systém – jedná se o primární IS sloužící pro hlavní činnost ZZ (správce), tj. pro poskytování následné zdravotní péče na území Pardubického kraje.
5. Vysokomýtská nemocnice – Nemocniční informační systém – jedná se o primární IS sloužící pro hlavní činnost ZZ (správce), tj. pro poskytování následné zdravotní péče na území Pardubického kraje.
6. Rehabilitační ústav Brandýs nad Orlicí – Nemocniční informační systém – jedná se o primární IS sloužící pro hlavní činnost ZZ (správce), tj. pro poskytování následné zdravotní péče na území Pardubického kraje.

Zabezpečením uvedených informačních a komunikačních systémů bude zajištěna kontinuita jejich provozu i v případě projevů kybernetických bezpečnostních událostí, tj. zamezení kybernetickým bezpečnostním incidentům, a tím bude zajištěno poskytování služeb veřejné správy ze strany zaměstnanců poskytovatelů ZS Pardubického kraje s využitím těchto IS.

Zvýšením kybernetické bezpečnosti v případě projevů kybernetických bezpečnostních událostí a zamezení kybernetickým bezpečnostním incidentům jak v době míru, tak v případě mimořádných událostí a krizových situací bude výrazně sníženo riziko omezení provozuschopnosti IS poskytovatelů ZS Pardubického kraje vyplývajících z projevů kybernetických rizik (kybernetických bezpečnostních událostí).

Zvýšením bezpečnosti bude dosaženo nejen garantované provozování uvedených IS, ale bude zajištěna vyšší ochrana zpracovávaných osobních údajů v souladu s legislativou ČR a EU. Opatření v rámci projektu a souvisejících aktivitách budou sloužit i jako opatření v návaznosti na Nařízení evropského parlamentu a rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR).

Předmět plnění (dílo) je detailně popsán v kap. 4 – Rozsah dodávky a souvisejících služeb.

Požadavky na servisní služby k tomuto Dílu jsou definovány v samostatném dokumentu, který je v rámci VZ samostatnou přílohou ZD a současně se stane přílohou Servisní smlouvy.

2 ČLENĚNÍ DOKUMENTU

Tento dokument obsahuje jen a pouze požadavky na dodávku a související služby (Dílo) a je členěn následovně:

- **Kapitola 3 – Předmět a rozsah dodávky~~Předmět a rozsah dodávky~~** – kapitola obsahuje požadavky na dodávky a služby (Dílo), které musí zhotovitel splnit ve svém řešení a ve své nabídce. Kapitola obsahuje základní koncept řešení, legislativní požadavky, konkrétní funkční a technické požadavky na řešení předmětu plnění v rámci VZ.
- **Kapitola 5 - Harmonogram~~Harmonogram~~** – kapitola obsahuje harmonogram realizace předmětu plnění VZ.
- **Kapitola 6 – Místa plnění~~Místa plnění~~** – kapitola obsahuje místa plnění v rámci realizace předmětu plnění VZ.
- **Kapitola 7 – Výchozí stav~~Výchozí stav~~** – kapitola obsahuje popis výchozího stavu pro realizaci předmětu VZ, tj. uvedení seznamu dotčených subjektů, jejich vztah k předmětu VZ, informační a komunikační technologie a vybavení, kterými subjekty disponují nebo které budou k dispozici pro realizaci VZ, případně další organizační a technické podmínky, které jsou důležité pro realizaci VZ.

Uvedené kapitoly a jejich obsah jsou uvedeny dále v tomto dokumentu.

Požadavky na servisní služby k tomuto Dílu jsou definovány v samostatném dokumentu, který v rámci VZ je přílohou ZD a současně se stane přílohou Servisní smlouvy.

3 PŘEDMĚT A ROZSAH DODÁVKY

Předmětem dodávky je komplexní dodávka a implementace technologií, dodávky SW, HW a infrastruktury pro realizaci technických bezpečnostních opatření dle § 5 odst. 3) zákona č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB) pro zabezpečení NIS provozovaných poskytovateli zdravotních služeb následné péče zřizovaných Pardubickým krajem (žadatel) v rámci výkonu veřejné správy v oblasti poskytování zdravotní péče, kterou Pardubický kraj vykonává na území Pardubického kraje.

Cílem projektu je zvýšení kybernetické bezpečnosti pro následující IS:

1. Léčebna dlouhodobě nemocných Rybitví – Nemocniční informační systém (NIS) – jedná se o primární IS sloužící pro hlavní činnost poskytovatele zdravotních služeb / příspěvkové organizace Pardubického kraje, tj. poskytování zdravotních služeb na území Pardubického kraje.
2. Odborný léčebný ústav Jevíčko – Nemocniční informační systém (NIS) – jedná se o primární IS sloužící pro hlavní činnost poskytovatele zdravotních služeb / příspěvkové organizace Pardubického kraje, tj. poskytování zdravotních služeb na území Pardubického kraje.
3. Albertinum, odborný léčebný ústav Žamberk – Nemocniční informační systém (NIS) – jedná se o primární IS sloužící pro hlavní činnost poskytovatele zdravotních služeb / příspěvkové organizace Pardubického kraje, tj. poskytování zdravotních služeb na území Pardubického kraje.
4. Nemocnice následné péče Moravská Třebová – Nemocniční informační systém (NIS) – jedná se o primární IS sloužící pro hlavní činnost poskytovatele zdravotních služeb / příspěvkové organizace Pardubického kraje, tj. poskytování zdravotních služeb na území Pardubického kraje.
5. Vysokomýtská nemocnice – Nemocniční informační systém (NIS) – jedná se o primární IS sloužící pro hlavní činnost poskytovatele zdravotních služeb / příspěvkové organizace Pardubického kraje, tj. poskytování zdravotních služeb na území Pardubického kraje.
6. Rehabilitační ústav Brandýs nad Orlicí – Nemocniční informační systém (NIS) – jedná se o primární IS sloužící pro hlavní činnost poskytovatele zdravotních služeb / příspěvkové organizace Pardubického kraje, tj. poskytování zdravotních služeb na území Pardubického kraje.

Detailní popis IS je uveden v kap. 7.2 – Informační systémy k zabezpečení.

Všichni uvedení poskytovatelé zdravotních služeb jsou malými organizacemi, tj. nemají dostatečnou odbornou kapacitu na řešení bezpečnostních opatření v potřebném rozsahu. Z tohoto důvodu bude část bezpečnostních opatření realizována společně s Nemocnicí Pardubického kraje a.s., která zajistí část sdílených služeb v oblasti kybernetické bezpečnosti pro všechny ostatní poskytovatele ZS. Jedná se např. o centrální LOGmanager, SIEM, analýzu síťového provozu a SOC. Cílem je tedy zajistit potřebné služby sdíleným způsobem, tj. splnění principu 3E, společné zajištění nedostatkové odborné kapacity a zaměření na společné zajištění provozu i kybernetické bezpečnosti v rámci všech poskytovatelů ZS na území Pardubického kraje.

Předmětem projektu je realizace následujících technických bezpečnostních opatření pro zabezpečení IS PAK (písmena odpovídají ZKB):

b) / § 18 nástroj pro ochranu integrity komunikačních sítí

c) / § 19 nástroj pro ověřování identity uživatelů

e) / § 21 nástroj pro ochranu před škodlivým kódem

g) / § 23 nástroj pro detekci kybernetických bezpečnostních událostí

h) / § 24 nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

k) / § 27 nástroj pro zajišťování úrovně dostupnosti informací

Rozsah dodávky je uveden v následující kapitole.

4 ROZSAH DODÁVKY A SOUVISEJÍCÍCH SLUŽEB

4.1 VYMEZENÍ PŘEDMĚTU A ROZSAHU DODÁVKY

Rozsah dodávky je následující:

#	Položka rozpočtu	Počet	Stručný popis položky	ID[1]
1	**Pardubický kraj**			
1.1	Rozšíření systému pro sběr a analýzu logů v NPK	1 soubor	Dodávka doplnění nebo rozšíření systému pro centrální sběr a analýzu logů z jednotlivých ZZ umístěný do NPK. Jedná se o doplnění nebo rozšíření stávajícího systému LOGmanager-XL o potřebnou kapacitu, licence a související služby pro sběr logů z nástrojů pro sběr a analýzu logů ze zapojených ZZ. Součástí je dodávka, instalace, nastavení, implementace nastavení a pravidel a napojení ZZ na tento systém a související služby. Popis požadavků na předmět plnění je uveden v kap. 4.4.3.1.	1.1 1.2
1.2	Zpracování událostí z analýzy síťového provozu ZZ v NPK	1 soubor	Nastavení centrálního zpracování a vyhodnocování událostí z analýzy síťového provozu (z firewalů) na straně ZZ předávány ve FortiAnalyzeru v NPK. Součástí je dodávka, instalace, nastavení, implementace nastavení a pravidel a napojení ZZ na tento systém a související služby. Popis požadavků na předmět plnění je uveden v kap. 4.4.3.2.	1.1 1.2
1.3	Zpracování událostí ze skenování perimetru ZZ v NPK	1 soubor	Nastavení centrálního zpracování a vyhodnocování událostí ze skenování perimetru na straně ZZ předávány ve FlowMon v NPK. Součástí je dodávka, instalace, nastavení, implementace nastavení a pravidel a napojení ZZ na tento systém a související služby. Logy budou předávány do LOGmanageru samostatně (viz výše). Popis požadavků na předmět plnění je uveden v kap. 4.4.3.3.	1.1 1.2

[1] Jedná se o pomocné interní označení příslušnosti do položky v rozpočtu projektu bez specifického významu pro VZ.

#	Položka rozpočtu	Počet	Stručný popis položky	ID[1]
2	**Léčebna dlouhodobě nemocných Rybitví (LDN Rybitví)**			
2.1	Nástroje monitorování a bezpečnost počítačových sítí	1 soubor	Nástroje monitorování a bezpečnost počítačových sítí (NetFlow). Včetně implementace, nastavení a uvedení do provozu. Popis požadavků na předmět plnění je uveden v kap. 4.4.4.1.	2.2
2.2	Nástroje pro ochranu síťového perimetru	1 soubor	Nástroje pro ochranu síťového perimetru (NGFW), v redundantním zapojení, včetně předávání dat do centrálního systému pro analýzu a vyhodnocení dat v NPK. Včetně implementace, nastavení a uvedení do provozu. Popis požadavků na předmět plnění je uveden v kap. 4.4.4.2.	2.3
2.3	Redundantní infrastruktura pro záložní DC pro provoz zabezpečovaného IS – HW	1 soubor	Redundantní infrastruktura pro záložní DC pro provoz zabezpečovaného IS v redundantním/vysoce dostupném režimu a zálohování dat IS, tj. dodávka serverů a datových úložišť pro provoz zabezpečovaného IS v záložní lokalitě a zajištění zálohování. Popis požadavků na předmět plnění je uveden v kap. 4.4.4.5.	2.4
2.4	Systémový SW pro redundantní infrastrukturu pro záložní DC pro provoz zabezpečovaného IS – SW	1 soubor	Systémový SW pro redundantní infrastrukturu pro záložní DC pro provoz zabezpečovaného IS v redundantním/vysoce dostupném režimu a zálohování dat IS, tj. dodávka technologií (virtualizace, OS, DB, zálohování atd.) pro servery a datová úložiště pro provoz zabezpečovaného IS v záložní lokalitě a zajištění zálohování. Popis požadavků na předmět plnění je uveden v kap. 4.4.4.5.	2.5
2.5	Dodávka Anti-X řešení pro ochranu před škodlivým kódem	1 soubor	Dodávka Anti-X řešení pro ochranu před škodlivým kódem pro ochranu aktiv zabezpečovaného IS, infrastruktury a pracovních stanic. Popis požadavků na předmět plnění je uveden v kap. 4.4.4.3.	2.6
2.6	Nástroje pro sběr logů a významných provozních událostí	1 soubor	Nástroje pro sběr logů a významných provozních událostí, základní vyhodnocení (Log Manager), včetně jejich předání do SOC NPK. Včetně implementace, nastavení a uvedení do provozu. Popis požadavků na předmět plnění je uveden v kap.	2.7

#	Položka rozpočtu	Počet	Stručný popis položky	ID[1]
			4.4.4.4.	
2.7	Infrastruktura pro provoz bezpečnostních technologií	1 soubor	Infrastruktura pro provoz bezpečnostních technologií, tj. dodávka serveru a datových úložišť pro nástroje pro sběr logů a významných provozních událostí. Popis požadavků na předmět plnění je uveden v kap. 4.4.4.5.	2.8
2.8	Systémový SW pro provoz bezpečnostních technologií	1 soubor	Systémový SW pro provoz bezpečnostních technologií, tj. dodávka technologií (virtualizace, OS, DB atd.) pro serveru a datová úložiště pro nástroje pro sběr logů a významných provozních událostí. Popis požadavků na předmět plnění je uveden v kap. 4.4.4.5.	2.9
3	**Odborný léčebný ústav Jevíčko (OLU Jevíčko)**			
3.1	Nástroje pro ochranu síťového perimetru a vnitřní sítě	1 soubor	Nástroje pro ochranu síťového perimetru (NGFW), v redundantním zapojení a FW pro zabezpečení vnitřní sítě (včetně WiFi), včetně předávání dat do centrálního systému pro analýzu a vyhodnocení dat v NPK. Včetně implementace, nastavení a uvedení do provozu. Popis požadavků na předmět plnění je uveden v kap. 4.4.5.1.	3.2
3.2	Nástroje monitorování a bezpečnost počítačových sítí	1 soubor	Nástroje monitorování a bezpečnost počítačových sítí (FlowMon). Včetně implementace, nastavení a uvedení do provozu. Popis požadavků na předmět plnění je uveden v kap. 4.4.5.2.	3.3
3.3	Dvoufaktorová autentizace administrátorských VPN přístupů	1 soubor	Dvoufaktorová autentizace administrátorských VPN přístupů. Včetně implementace, nastavení a uvedení do provozu. Popis požadavků na předmět plnění je uveden v kap. 4.4.5.3.	3.4
3.4	Zálohovací infrastruktura pro záložní DC pro zálohování dat a technologií zabezpečovaného IS – HW	1 soubor	Zálohovací infrastruktura pro záložní DC pro zálohování dat a technologií zabezpečovaného IS, tj. dodávka datových úložišť pro zálohování zabezpečovaného IS v záložní lokalitě a zajištění zálohování. Popis požadavků na předmět plnění je uveden v kap. 4.4.5.4.	3.5

#	Položka rozpočtu	Počet	Stručný popis položky	ID[1]
3.5	Nástroje pro sběr logů a významných provozních událostí	1 soubor	Nástroje pro sběr logů a významných provozních událostí, základní vyhodnocení (Log Manager), včetně jejich předání do SOC NPK. Včetně implementace, nastavení a uvedení do provozu. Popis požadavků na předmět plnění je uveden v kap. 4.4.5.5.	3.6
3.6	Infrastruktura pro provoz bezpečnostních technologií	1 soubor	Infrastruktura pro provoz bezpečnostních technologií, tj. dodávka serveru a datových úložišť pro nástroje pro sběr logů a významných provozních událostí. Popis požadavků na předmět plnění je uveden v kap. 4.4.5.6.	3.7
3.7	Systémový SW pro provoz bezpečnostních technologií	1 soubor	Systémový SW pro provoz bezpečnostních technologií, tj. dodávka technologií (virtualizace, OS, DB atd.) pro serveru a datová úložiště pro nástroje pro sběr logů a významných provozních událostí. Popis požadavků na předmět plnění je uveden v kap. 4.4.5.6.	3.8
4	**Albertinum, odborný léčebný ústav Žamberk (OLÚ Albertinum Žamberk)**			
4.1	Nástroje pro ochranu síťového perimetru	1 soubor	Nástroje pro ochranu síťového perimetru (NGFW), v redundantním zapojení, včetně předávání dat do centrálního systému pro analýzu a vyhodnocení dat v NPK. Nástroje monitorování a bezpečnost počítačových sítí. Včetně implementace, nastavení a uvedení do provozu. Popis požadavků na předmět plnění je uveden v kap. 4.4.6.1 a kap. 4.4.6.4.	4.3
4.2	Redundantní infrastruktura pro záložní DC pro provoz zabezpečovaného IS – HW	1 soubor	Redundantní infrastruktura pro záložní DC pro provoz zabezpečovaného IS v redundantním/vysoce dostupném režimu a zálohování dat IS, tj. dodávka serverů, UPS pro páteřní síťové prvky a pro bronchoskopický sál a datových úložišť (archivační úložiště pro EZD) pro provoz zabezpečovaného IS v záložní lokalitě a zajištění zálohování. Popis požadavků na předmět plnění je uveden v kap. 4.4.6.2.	4.4
4.3	Systémový SW pro redundantní infrastrukturu	1 soubor	Systémový SW pro redundantní infrastrukturu pro záložní DC pro provoz zabezpečovaného IS v redundantním/vysoce dostupném režimu a zálohování dat IS, tj. dodávka technologií (virtualizace, virtualizační HA	4.5

#	Položka rozpočtu	Počet	Stručný popis položky	ID[1]
	pro záložní DC pro provoz zabezpečovaného IS – SW		cluster, OS, DB, zálohování atd.) pro servery a datová úložiště pro provoz zabezpečovaného IS v záložní lokalitě a zajištění zálohování. Popis požadavků na předmět plnění je uveden v kap. 4.4.6.2.	
4.4	Dodávka Anti-X řešení pro ochranu před škodlivým kódem	1 soubor	Dodávka Anti-X řešení pro ochranu před škodlivým kódem pro ochranu aktiv zabezpečovaného IS, infrastruktury a pracovních stanic. Popis požadavků na předmět plnění je uveden v kap. 4.4.6.3.	4.6
4.5	Nástroje pro sběr logů a významných provozních událostí	1 soubor	Nástroje pro sběr logů a významných provozních událostí, základní vyhodnocení (Log Manager), včetně jejich předání do SOC NPK. Včetně implementace, nastavení a uvedení do provozu. Popis požadavků na předmět plnění je uveden v kap. 4.4.6.5.	4.7
4.6	Infrastruktura pro provoz bezpečnostních technologií	1 soubor	Infrastruktura pro provoz bezpečnostních technologií, tj. dodávka serveru a datových úložišť pro nástroje pro sběr logů a významných provozních událostí. Popis požadavků na předmět plnění je uveden v kap. 4.4.6.2.	4.8
4.7	Systémový SW pro provoz bezpečnostních technologií	1 soubor	Systémový SW pro provoz bezpečnostních technologií, tj. dodávka technologií (virtualizace, OS, DB atd.) pro serveru a datová úložiště pro nástroje pro sběr logů a významných provozních událostí. Popis požadavků na předmět plnění je uveden v kap. 4.4.6.2.	4.9
5	**Nemocnice následné péče Moravská Třebová (NNP Moravská Třebová)**			
5.1	Nástroje pro ochranu síťového perimetru	1 soubor	Nástroje pro ochranu síťového perimetru (NGFW), v redundantním zapojení, včetně předávání dat do centrálního systému pro analýzu a vyhodnocení dat v NPK. Včetně implementace, nastavení a uvedení do provozu. Popis požadavků na předmět plnění je uveden v kap. 4.4.7.1.	5.2
5.2	Nástroje pro identifikaci, autentizaci a řízení	1 soubor	Zavedení MS Active Directory pro identifikaci, autentizaci a řízení oprávnění uživatelů a administrátorů. Součástí bude napojení na NIS (zabezpečovaný systém) a další provozní	5.4

#	Položka rozpočtu	Počet	Stručný popis položky	ID[1]
	oprávnění uživatelů a administrátorů – SW		technologie a řízení oprávnění v MS AD. Součástí jsou licence OS, AD a zapojení v redundantním režimu. Popis požadavků na předmět plnění je uveden v kap. 4.4.7.2.	
5.3	Nástroje monitorování a bezpečnost počítačových sítí	1 soubor	Nástroje monitorování a bezpečnost počítačových sítí (FlowMon). Včetně implementace, nastavení a uvedení do provozu. Popis požadavků na předmět plnění je uveden v kap. 4.4.7.3.	5.5
5.4	Nástroje pro sběr logů a významných provozních událostí	1 soubor	Nástroje pro sběr logů a významných provozních událostí, základní vyhodnocení (Log Manager), včetně jejich předání do SOC NPK. Včetně implementace, nastavení a uvedení do provozu. Popis požadavků na předmět plnění je uveden v kap. 4.4.7.4.	5.6
5.5	Redundantní infrastruktura pro záložní DC pro provoz zabezpečovaného IS a bezpečnostních technologií – HW	1 soubor	Redundantní infrastruktura pro záložní DC pro provoz zabezpečovaného IS v redundantním/vysoce dostupném režimu a zálohování dat IS, tj. dodávka serverů, UPS, redundantních switchů a datových úložišť pro provoz zabezpečovaného IS v záložní lokalitě a zajištění zálohování. Popis požadavků na předmět plnění je uveden v kap. 4.4.7.5.	5.7
5.6	Systémový SW pro redundantní infrastrukturu pro záložní DC pro provoz zabezpečovaného IS a bezpečnostních technologií – SW	1 soubor	Systémový SW pro redundantní infrastrukturu pro záložní DC pro provoz zabezpečovaného IS v redundantním/vysoce dostupném režimu a zálohování dat IS, tj. dodávka technologií (virtualizace, OS, DB, zálohování atd.) pro servery a datová úložiště pro provoz zabezpečovaného IS v záložní lokalitě a zajištění zálohování. Popis požadavků na předmět plnění je uveden v kap. 4.4.7.5.	5.8
6	**Vysokomýtská nemocnice (NVM)**			
6.1	Rozšíření Anti-X řešení pro ochranu před	1 soubor	Rozšíření Anti-X řešení pro ochranu před škodlivým kódem pro ochranu aktiv zabezpečovaného IS, infrastruktury a pracovních stanic o podporu EDR.	6.2

#	Položka rozpočtu	Počet	Stručný popis položky	ID[1]
	škodlivým kódem		Popis požadavků na předmět plnění je uveden v kap. 4.4.8.1.	
6.2	Nástroje pro ochranu síťového perimetru	1 soubor	Nástroje pro ochranu síťového perimetru (NGFW), v redundantním zapojení, včetně předávání dat do centrálního systému pro analýzu a vyhodnocení dat v NPK. Včetně implementace, nastavení a uvedení do provozu. Popis požadavků na předmět plnění je uveden v kap. 4.4.8.2.	6.4
6.3	Nástroje pro segmentaci sítí a řízení přístupu k síti	1 soubor	Nástroje pro segmentaci sítí, oddělení podsítí, rozdělení sítí pro zaměstnance, pacienty a návštěvy, sandboxing, Implementace přístupů do LAN sítě (802.1x). Včetně implementace, nastavení a uvedení do provozu. Popis požadavků na předmět plnění je uveden v kap. 4.4.8.3.	6.5
6.4	Nástroje monitorování a bezpečnost počítačových sítí	1 soubor	Nástroje monitorování a bezpečnost počítačových sítí (FlowMon). Včetně implementace, nastavení a uvedení do provozu. Popis požadavků na předmět plnění je uveden v kap. 4.4.8.4.	6.6
6.5	Řízení přístupu uživatelů a administrátorů	1 soubor	Dvoufaktorová autentizace VPN přístupů s napojením na MS AD. Napojení MS AD na personální systémy s ukončováním přístupů v MS AD a navazujících systémech s ukončením pracovního poměru. Včetně implementace, nastavení a uvedení do provozu. Popis požadavků na předmět plnění je uveden v kap. 4.4.8.5.	6.7
6.6	Zálohovací infrastruktura pro záložní DC pro zálohování dat a technologií zabezpečovaného IS – HW	1 soubor	Zálohovací infrastruktura pro záložní DC pro zálohování dat a technologií zabezpečovaného IS, tj. dodávka datových úložišť a racku pro zálohování zabezpečovaného IS v záložní lokalitě a zajištění zálohování. Popis požadavků na předmět plnění je uveden v kap. 4.4.8.6.	6.8
6.7	Software pro zálohovací infrastrukturu pro záložní DC pro zálohování	1 soubor	Software pro zálohovací infrastrukturu pro záložní DC pro zálohování dat a technologií zabezpečovaného IS, tj. dodávka virtualizace, operační systémů a zálohovacích technologií pro zálohování zabezpečovaného IS v záložní lokalitě a zajištění zálohování.	6.9

#	Položka rozpočtu	Počet	Stručný popis položky	ID[1]
	dat a technologií zabezpečovaného IS – SW		Popis požadavků na předmět plnění je uveden v kap. 4.4.8.6.	
6.8	Nástroje pro sběr logů a významných provozních událostí	1 soubor	Nástroje pro sběr logů a významných provozních událostí, základní vyhodnocení (Log Manager), včetně jejich předání do SOC NPK. Včetně implementace, nastavení a uvedení do provozu. Popis požadavků na předmět plnění je uveden v kap. 4.4.8.7.	6.10
6.9	Infrastruktura pro provoz bezpečnostních technologií	1 soubor	Infrastruktura pro provoz bezpečnostních technologií, tj. dodávka serveru a datových úložišť pro nástroje pro sběr logů a významných provozních událostí. Popis požadavků na předmět plnění je uveden v kap. 4.4.8.8.	6.11
6.10	Systémový SW pro provoz bezpečnostních technologií	1 soubor	Systémový SW pro provoz bezpečnostních technologií, tj. dodávka technologií (virtualizace, OS, DB atd.) pro serveru a datová úložiště pro nástroje pro sběr logů a významných provozních událostí. Popis požadavků na předmět plnění je uveden v kap. 4.4.8.8.	6.12
7	**Rehabilitační ústav Brandýs nad Orlicí (RÚ BnO)**			
7.1	Nástroje pro ochranu síťového perimetru	1 soubor	Nástroje pro ochranu síťového perimetru (NGFW), v redundantním zapojení, včetně předávání dat do centrálního systému pro analýzu a vyhodnocení dat v NPK. Včetně implementace, nastavení a uvedení do provozu. Popis požadavků na předmět plnění je uveden v kap. 4.4.9.1.	7.2
7.2	Nástroje monitorování a bezpečnost počítačových sítí	1 soubor	Nástroje monitorování a bezpečnost počítačových sítí (FlowMon). Včetně implementace, nastavení a uvedení do provozu. Popis požadavků na předmět plnění je uveden v kap. 4.4.9.2.	7.3
7.3	Redundantní infrastruktura pro záložní DC pro provoz	1 soubor	Redundantní infrastruktura pro záložní DC pro provoz zabezpečovaného IS v redundantním/vysoce dostupném režimu a zálohování dat IS, tj. dodávka serverů a datových úložišť pro provoz zabezpečovaného IS v záložní lokalitě a zajištění zálohování.	7.4

#	Položka rozpočtu	Počet	Stručný popis položky	ID[1]
	zabezpečované ho IS – HW		Popis požadavků na předmět plnění je uveden v kap. 4.4.9.3.	
7.4	Systémový SW pro redundantní infrastrukturu pro záložní DC pro provoz zabezpečované ho IS – SW	1 soubor	Systémový SW pro redundantní infrastrukturu pro záložní DC pro provoz zabezpečovaného IS v redundantním/vysoce dostupném režimu a zálohování dat IS, tj. dodávka technologií (virtualizace, OS, DB, zálohování atd.) pro servery a datová úložiště pro provoz zabezpečovaného IS v záložní lokalitě a zajištění zálohování. Popis požadavků na předmět plnění je uveden v kap. 4.4.9.3.	7.5
7.5	Nástroje pro sběr logů a významných provozních událostí	1 soubor	Nástroje pro sběr logů a významných provozních událostí, základní vyhodnocení (Log Manager), včetně jejich předání do SOC NPK. Včetně implementace, nastavení a uvedení do provozu. Popis požadavků na předmět plnění je uveden v kap. 4.4.9.4.	7.6
7.6	Infrastruktura pro provoz bezpečnostních technologií	1 soubor	Infrastruktura pro provoz bezpečnostních technologií, tj. dodávka serveru a datových úložišť pro nástroje pro sběr logů a významných provozních událostí. Popis požadavků na předmět plnění je uveden v kap. 4.4.9.3.	7.7
7.7	Systémový SW pro provoz bezpečnostních technologií	1 soubor	Systémový SW pro provoz bezpečnostních technologií, tj. dodávka technologií (virtualizace, OS, DB atd.) pro serveru a datová úložiště pro nástroje pro sběr logů a významných provozních událostí. Popis požadavků na předmět plnění je uveden v kap. 4.4.9.3.	7.8
8	**Ostatní systémy a technologie**			
8.1	Nástroje pro penetrační testy a penetrační testy	5 ks	Testy zranitelnosti včetně nástrojů pro opakované provádění testování zranitelnosti v rámci udržitelnosti. Popis požadavků na předmět plnění je uveden v kap. 4.4.10.1.	V.2

Tabulka 2: Předmět a rozsah dodávky

4.1.1 Související služby a náležitosti dodávky

Součástí dodávky jsou dále následující služby a náležitosti:

1. Projektové řízení dodávky řešení

2. Zpracování návrhu dodávky a konfigurace technických opatření v souladu s výstupy a doporučeními vyplývající z bezpečnostního auditu (výstupy budou poskytnuty v rámci součinnosti pouze vybranému dodavateli), související konzultace.
3. Dodávka, implementace, instalace, zapojení a konfigurace technických opatření v souladu s výstupy a doporučeními vyplývající z bezpečnostního auditu.
4. Migrace vybraných systémů (NIS) a technologií (bezpečnostní technologie) na novou infrastrukturu.
5. Konfigurační změny zabezpečovaných IS a implementace změn informačních systémů a jejich součástí.
6. Ověření funkčnosti dodaných technologií, zabezpečovaných IS a jejich (sou)částí.
7. Úpravy nastavení bezpečnostních technologií na základě výstupů z testování zranitelnosti / penetračních testů.
8. Dodávka dokumentace dodaného vybavení a jeho částí (min. administrátorská dokumentace, dokumentace skutečného provedení/stavu po implementaci, systémová dokumentace, zpracování bezpečnostní dokumentace včetně hodnocení aktiv a rizik). Dokumentace může být jedním dokumentem, nicméně musí obsahovat všechny relevantní informace.
9. Poskytnutí informací pro zpracování nebo aktualizaci bezpečnostní dokumentace včetně hodnocení aktiv a rizik s tím, že bezpečnostní dokumentace by měla plně reflektovat veškeré technologické a funkční změny.
10. Seznámení s obsluhou dodávaného systému a jeho budoucím provozem (správci).
11. Zařazení do provozního prostředí objednatele (dohled, zálohování apod.).
12. Provedení zkušebního provozu.
13. Poskytnutí záruky min. 5 roky na vybavení v rámci technických opatření.

Doplňující požadavky na implementaci:

1. Zajištění kontinuity provozu poskytovatelů ZS Pardubického kraje a NPK. Po stránce nepřetržitého provozu se předpokládají pouze plánované odstávky dotčených IS a technologií, a to pouze na nezbytnou dobu.
2. Požaduje se kontinuita nastavených parametrů IS a existujících technologií a jiných aspektů provozu. Nepředpokládá investici do opětovného zadávání a pořizování těchto údajů.

4.1.2 Dodávkou nedotčené oblasti stávajícího řešení

Dodávkou nebudou dotčeny následující oblasti stávajícího řešení:

1. Současné systémy, technologie a poskytovatelů ZS zůstanou zachovány a nebudou negativně dotčeny realizací projektu.

4.1.3 Vyloučení z dodávky

Předmětem dodávky není:

1. Zajištění v rámci požadavků neuvedené komunikační infrastruktury (sítě apod.) mezi jednotlivými prvky systému.
2. Infrastruktura, HW a systémový SW poskytovaný Objednatelem (PAK a jeho ZZ) uvedený ve výchozím stavu a neuvedený v požadavcích.
3. Spotřební materiál využívaný v následném provozu informačních systémů a technologií neuvedený v rámci požadavků.

Koncept řešení, principy a požadavky na dodávky a služby jsou uvedeny dále v tomto dokumentu.

4.2 VÝCHODISKA A PŘIPRAVENOST

Pro řešení jsou stanovena následující východiska:

#	Popis východiska
1.	Připravenost datových center bude zajištěna min. v následujícím rozsahu: 1. Dostatečně kapacitní napájení datových center pro umístění technologií. 2. Klimatizace v datových centrech. 3. Strukturovaná kabeláž v rámci DC, mezi DC a mezi dodávanými technologiemi a zabezpečovanými IS. 4. Napojení na ostatní komunikační technologie.
2.	Nutnost zajištění ochrany osobních údajů a bezpečnosti v souladu s legislativou a moderními principy – Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob (GDPR), zákona č. 181/2014 Sb. – Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a požadavky kladené na KII.
3.	Soulad se SMĚRNICÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)

Tabulka 3: Východiska

Další východiska jsou definována výchozím stavem uvedeným v kap. 7 – Výchozí stav.

4.3 ZÁKLADNÍ POŽADAVKY NA ZABEZPEČENÍ IS

Základní požadavky na požadované řešení jsou následující:

1. Předmětem je zabezpečení informačních systémů uvedených v kap. 1 tohoto dokumentu.
2. Budou zajištěny všechny současné integrace uvedených IS a vazby na jiné IS a technologie nezbytné pro provoz dotčených poskytovatelů zdravotních služeb.
3. Dodávané technologie musí plnit podmínky legislativy a norem uvedených v kap 4.2.
4. Izolovanost informačních systémů – přístup do systémů a přístup ze systémů ven je možný pouze přes definované přístupové body.
5. Vysoká dostupnost bezpečnostních technologií.

Detailní popis požadavků na dodávky je uveden v následující kapitole.

4.4 POŽADAVKY NA DODÁVKY

V této kapitole jsou uvedeny požadavky na dodávky.

4.4.1 Obecné a společné požadavky

V této kapitole jsou uvedeny obecné požadavky na požadované řešení:

#	Požadavek
P.1	Dodávané technologie musí svojí architekturou splňovat obecné zásady informační bezpečnosti v míře, odpovídající charakteru užití a kategorii zpracovávaných dat (GDPR).
P.2	Veškeré nabízené SW i HW prvky musí být plně kompatibilní se stávajícími systémy a technologiemi ZZ PAK a NPK.

#	Požadavek
P.3	Součástí implementace musí být i veškeré potřebné licence a služby nezbytné pro dodávku a provoz dodávaných technologií min. po dobu účinnosti servisní smlouvy.
P.4	Zaručená perspektiva rozvoje a podpory je minimálně po dobu dalších 6 let od uvedení do provozu.
Legislativa a další normy	
P.5	Soulad s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob (GDPR – General Data Protection Regulation) v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
P.6	Soulad se Zákonem č. 181/2014 Sb., o kybernetické bezpečnosti v aktuálním znění a vyhláškou Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti v aktuálním znění. Je připravována nová vyhláška o kybernetické bezpečnosti. Pokud nabude platnosti v době realizace dodávky, je požadován i soulad s touto vyhláškou.
P.7	Soulad s prováděcím nařízením Komise (EU) 2018/151 ze dne 30. ledna 2018, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný (dále jen „PNK“).
P.8	Soulad se SMĚRNICÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2).
P.9	Pokud výrobce nabízených technologií dodává specifické technologie pro specifické trhy (český, resp. trh EU), musí být nabízená technologie určená pro trh relevantní pro objednatele a jeho ZZ (český, resp. trh EU). HW a SW licence a jejich PN (produktové číselné označení) musí být dostupné přímo v oficiálním ceníku výrobce pro relevantní trh a licencován a určen (registrován) přímo pro PAK, resp. pro jeho ZZ. Podpora na licence ve všech úrovních musí být zajištěna přímo jejich výrobcem, kterého může Zadavatel přímo kontaktovat.

Tabulka 4: Obecné a společné požadavky

Pro konkrétní oblasti jsou uvedeny specifické požadavky samostatně v dílčích podkapitolách.

4.4.2 Společné technologie

V této kapitole jsou uvedeny požadavky na dodávky společných technologií.

Společnými technologiemi jsou míněny technologie, které jsou požadovány pro více ZZ PAK a z důvodu jejich propojení musí být tyto technologie kompatibilní, tj. jejich základní požadavky jsou stejné.

4.4.2.1 Nástroje pro sběr logů a významných provozních událostí

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.10	Dodávka systému pro centralizovanou správu logů a jiných strojových dat z libovolných zdrojů (OS, DB, virtualizace, komunikační infrastruktura, IS). Sběr, dlouhodobé nezpochybnitelné ukládání a analýza zdrojových logů/dat. Systém musí umožňovat prohledávat agregovaná data v reálném čase, vytvářet analýzy, reporty a upozornění na události korelované z dat více zdrojů. Soulad s požadavky zákonných norem – shoda s ČSN/ISO 27001:2013 o pořizování auditních záznamů (na vyžádání musí dodavatel předložit potvrzení o shodě), plnění požadavků GDPR a Zákona o kybernetické bezpečnosti.
P.11	Minimální požadavky na dodávaný systém/nástroj: 1. Podporované standardy pro záznamy činnosti: CEF, LEEF, RSYSLOG, SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP 2. Min. podporované IT platformy pro sběr událostí: HPE/Aruba, Fortinet, Flowmon, APC, MS Windows servery a stanice, Linux servery, MS SQL Server, virtualizace VMware a Hyper-V. 3. Podpora šifrované komunikace (TLS) při přenášení záznamů do SIEM 4. Kapacita databáze: min. 12 TB 5. Síťové porty min. 4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW 6. Konfigurace všech parametrů síťového rozhraní včetně link agregace dle LACP (802.3ad) 7. Trvalá rychlost zpracovávání záznamů: 2000 EPS (událostí/s) 8. Definice alertů a jejich zasílání min. prostřednictvím e-mail zpráv 9. Systém umožňuje vytvořit uživatelsky definované parsery bez nutnosti spolupráce s výrobcem nebo dodavatelem. Pro vytváření parserů nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. 10. Jednotná centrální webová konzole s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. 11. Podpora multitenantního prostředí. 12. V rámci dodaného systému neexistují licenční omezení na počet připojených zdrojů záznamů (logů), objem sbíraných dat, dobu jejich uchování ani na rychlost jejich sběru. 13. Zařízení je funkční po celou dobu jeho životnosti bez nutnosti ročních licenčních poplatků za údržbu. 14. Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky.

#	Požadavek
	15. Historická data v požadované délce retence uložená v systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy správce. 16. Vybrané logy lze dále přeposílat na existující centrální LOGmanager v NPK pro centrální zpracování. 17. Možnost nasazení v režimu vysoké dostupnosti.
P.12	Události z prostředí MS Windows jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních Windows logů (Aplikace, Zabezpečení, Instalace, Systém), tak monitoring textových souborových logů (min. Protokoly aplikací a služeb). Agent musí mít možnost automatické instalace prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému. Filtrace odesílaných událostí agentem se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole systému. Logy nastavené k filtraci jsou filtrovány na straně Windows agenta a nejsou nijak odesílány po síti. Licence na využití agentů musí pokrýt veškeré současné i budoucí systémy s OS Windows či Windows Server bez nutnosti dodatečných finančních nákladů.
P.13	Zobrazování, vyhledávání a reporting: 1. Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění. 2. Systém umožňuje snadné vyhledávání a filtrování událostí dle více kritérií. 3. Filtry musejí umožňovat okamžitě testovat jejich účinnost a zobrazit kolik z uložených dat zvolený filtr zasáhne a kolik logů by případně filtroval minimálně za posledních 24 hodin. 4. Vizuální programovací jazyk není prezentován textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. 5. Systém musí umožňovat konfiguraci filtrace nerelevantních událostí v grafickém rozhraní vizuálního programovacího jazyka. Pro psaní filtrace nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. 6. Definice reportů a jejich pravidelné generování a zasílání prostřednictvím e-mail zpráv. 7. Systém obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Pro vytváření nových pohledů na data není přípustné používat povinně SQL jazyk. 8. Možnost vytváření grafických reportů (i ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj musí být integrální součástí dodávaného systému a musí se obsluhovat v jednotném rozhraní nabízeného produktu. 9. Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. 10. Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování.
P.14	Systém musí umožnit vytváření uživatelských rolí definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentům systému.

#	Požadavek
	Systém musí podporovat ověřování uživatele systému na externím LDAP / MS AD serveru. V případě výpadku externího LDAP / MS AD systému musí podporovat ověření lokálního účtu.
P.15	Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem.
P.16	Vybrané logy budou dále automatizovaně předávány do centrálního LOGmanager v NPK, kde bude dále vyhodnocen a případně zpracováno ze strany SOC. Předávání logů do centrálního LOGmanageru v NPK je předmětem dodávky, tj. musí být dodány nástroje pro garantované automatizované předávání logů do centrálního LOGmanageru v NPK.
P.17	Pokud se není zařízení komplexním systémem (all-in-one) obsahující veškerý HW, systémový SW a vlastní nástroje, musí být potřebná provozní infrastruktura a systémový SW dodány v samostatné položce specifické pro poskytovatele ZS (server, diskové pole).
P.18	Součástí předmětu plnění je dodávka, instalace, implementace, licence, konfigurace pro místní podmínky poskytovatele ZS, ověření funkčnosti (lokání, i předávání dat do NPK), dokumentace.
P.19	Podpora výrobce v režimu min. 8x5 NBD včetně nároku na nejnovější firmware a subskripce (pokud budou vydávány) po dobu min. 5 let.

Tabulka 5: Nástroje pro sběr logů a významných provozních událostí

4.4.2.2 Nástroje monitorování a bezpečnost počítačových sítí

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.20	Je požadováno řešení umožňující dlouhodobé real-time monitorování sítě na bázi technologie NetFlow pro automatické vyhodnocování IP toků provádějící automatickou detekci bezpečnostních nebo provozních anomálií datové sítě (ADS) a jejich hlášení formou událostí.
P.21	Systém založen na pokročilých metodách tzv. behaviorální analýzy, které umožňují odhalovat hrozby a incidenty, které překonaly zabezpečení na perimetru nebo bezpečnostní ochranu koncových stanic, a pro které dosud není dostupná signatura.
P.22	Požaduje se dodávka sond pro monitorování provozu v rámci počítačové sítě, vytváření statistik v podobě IP toků a zasílání (případně exportu), možnost uložení k další analýze kolektorovou aplikací kompatibilní s NetFlow/IPFIX standardem. statistiky umožňující monitorování provozu na síti pro zajištění její bezpečnosti a řešení provozních problémů.
P.23	Minimálními požadavky: 1. Propustnost min 3 Mpps 2. Podporovaný standard pro sběr toků: IPFIX, NetFlow v5 a v9, NetStream, jFlow, cflowd, podpora IPv4 a Ipv6 3. Podpora L3 4. Podpora externích služeb (reputation databases, indicators of compromise), whois, IP tools, weblinks 5. Behaviorální analýza / detekce pomocí machine learning, adaptive baselining, behaviorální analýzy, heuristik

#	Požadavek
	6. Integrovaná funkce IDS 7. Klasifikace incidentů 8. Reakce na události formou definovaných alertů pomocí e-mail, PDF/CSV, SYSLOG, SNMP, packet capture trigger, script trigger 9. Definice reportů a jejich pravidelné generování a zasílání prostřednictvím e-mail zpráv 10. Podpora multitenantního prostředí 11. Podporované standardy pro záznamy činnosti: CEF, SYSLOG 12. Počet zpracovaných toků pomocí behaviorální analýzy: min. 1000 flow/s 13. Počet a přenosová rychlost síťových rozhraní pro sběr dat: 4 x 10/100/1000 Mbps 14. Možnost dohledání libovolné komunikace až na úroveň jednotlivých flow záznamů 15. Pokročilá analýza chování k detekci nežádoucích anomálií v síťovém provozu (ADS) 16. Dashboard poskytující rychlý přehled o nejnovějších událostech, celkových statistikách událostí nebo využívaných a poskytovaných službách. 17. Zaznamenávání událostí do SIEM pomocí formátu CEF, SNMP trap 18. Vizualizace událostí ve formě stromu událostí, časové posloupnosti, poskytnutí detailu a zachyceného flow jako důkazu 19. Redundantní řešení
P.24	Pokud se není zařízení komplexním systémem (all-in-one) obsahující veškerý HW, systémový SW a vlastní nástroje, musí být potřebná provozní infrastruktura a systémový SW dodány v samostatné položce specifické pro poskytovatele ZS.
P.25	Předávání událostí do nástroje pro sběr logů a významných provozních událostí, který je předmětem dodávky.
P.26	Součástí předmětu plnění je dodávka, instalace, implementace, licence, konfigurace pro místní podmínky poskytovatele ZS, ověření funkčnosti (lokání, i předávání dat do NPK), dokumentace.
P.27	Podpora výrobce v režimu min. 8x5, NBD včetně nároku na nejnovější firmware a subskripce (pokud budou vydávány) po dobu min. 5 let.

Tabulka 6: Nástroje monitorování a bezpečnost počítačových sítí

4.4.3 Pardubický kraj

V této kapitole jsou uvedeny požadavky na dodávky pro: Pardubický kraj.

4.4.3.1 Rozšíření systému pro sběr a analýzu logů v NPK (1.1)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

4.4.3.1.1 Výchozí stav

Nemocnice Pardubického kraje a.s. (NPK) není příjemcem ani uživatelem dodávek v rámci řešení projektu.

NPK bude v rámci dohody mezi Pardubickým krajem (zakladatel) a NPK poskytovat některé služby v rámci kybernetické bezpečnosti pro ostatní poskytovatele zdravotních služeb zřizovaných Pardubickým krajem. Tito poskytovatelé ZS budou uživatelé pořízeného vybavení a budou využívat služby NPK v případech, kdy nejsou dostatečně kapacitně a kvalifikačně vybavení pro zajištění služeb v oblasti kybernetické bezpečnosti.

Následující text uvádí relevantní stav a připravované aktivity na straně NPK, které jsou relevantní pro tento projekt.

LOGmanager

NPK disponuje technologií LOGmanager-XL od firmy LOGmanager, technologie byla pořízena v roce 2020.

V této technologii jsou uloženy logy a je nad nimi prováděna základní analýza.

V rámci projektu se předpokládá, že vybrané logy od poskytovatelů ZS (z jejich kolektovacích logovacích nástrojů) budou předávány do LOGmanager-XL v NPK, kde budou dále zpracovávány. Data/logy jednotlivých poskytovatelů ZS zůstanou uložená i v jejich lokálních kolektovacích nástrojích.

V rámci dodávky musí být pořízena nová disková kapacita pro ukládání logů od poskytovatelů ZS nad rámec kapacity využívané ze strany NPK, která je již nyní téměř spotřebovaná, data jsou uchovávána po dobu 18 měsíců. Pokud by nebylo možné rozšířit stávající LOGmanager-XL v NPK, je předmětem dodávky centrální nástroj pro sběr a vyhodnocení logů a významných provozních událostí sesbíraných od jednotlivých zapojených provozovatelů ZS.

Rozšířená analýza bude prováděna v SIEM, nikoliv v tomto nástroji (viz dále).

SIEM

NPK nyní neprovozuje SIEM, nicméně plánuje jeho pořízení, zvažujte technologii QRADAR, nicméně technologie vyplyne z výběrového řízení.

Do SIEM budou předávány logy a události z jednotlivých kolektovacích logovacích nástrojů ZZ a vyhodnocovány.

Výstupy ze SIEM budou zpracovávány v rámci SOC.

SOC

NPK plánuje zřízení SOC, a to buď vlastními prostředky (pokud budou k dispozici dostatečné personální zdroje) nebo nákup této služby externě (pokud nebudou dostupné zdroje pro provoz).

Služba bude využívána i pro potřeby ZZ, kdy jim bude poskytovat upozorňování na události vyžadujících řešení. Neočekávají se přímé zásahy do prostředí ZZ ze strany SOC, zásahy budou prostřednictvím administrátorů na straně ZZ, případně jejich smluvních partnerů poskytujících servisní služby.

4.4.3.1.2 Požadavky na řešení

#	Požadavek
P.28	Dodávka systému pro centrální sběr a analýzu logů z jednotlivých ZZ umístěný do NPK. Jedná se o doplnění, rozšíření stávajícího systému nebo dodávka nového systému a propojení do stávajícího systému LOGmanager-XL o potřebnou kapacitu, licence a související služby pro sběr logů z nástrojů pro sběr a analýzu logů ze zapojených ZZ.
P.29	Minimální požadavky na dodávku: 1. Možnost škálovatelného navýšení kapacity úložiště na základě licence 2. Integrace s NGFW, tzn. že data se přenáší z firewallu na logovací a reportovací platformu (kompatibilita s NGFW, které jsou součástí dodávky) 3. Podpora pro SYSLOG kompatibilní zařízení 4. Výkon logování: min. 6 GB / den 5. Kapacita storage (uložení historických dat): min. 3 TB 6. Real-time prohledávání logovaných dat 7. Vyhledávání historických dat podle typu události nebo typu provozu 8. Funkce zpětné kontroly logů o přístupu na web (až 7 dní) z důvodu „zero-day“ malicious websites

#	Požadavek
	9. Korelace logů 10. Vyhledávání podle zařízení 11. Uživatelská definice reportů (vzhled, obsah apod.) 12. Automatické generování reportů v daném čase a periodě 13. Automatické odesílání reportů emailem 14. Kompatibilní s nástroji pro sběr logů a významných provozních událostí jednotlivých poskytovatelů ZS (viz kap. 4.4.2.1)
P.30	Příjem logů a významných provozních událostí z dodávaných nástrojů sběr logů a významných provozních událostí jednotlivých poskytovatelů ZS (viz kap. 4.4.2.1).
P.31	Pokud se není zařízení komplexním systémem (all-in-one) obsahující veškerý HW, systémový SW a vlastní nástroje (např. se jedná o virtuální appliance), musí být potřebná provozní infrastruktura a systémový SW dodány v samostatné položce specifické pro poskytovatele ZS.
P.32	Součástí předmětu plnění je dodávka, instalace, implementace, licence, konfigurace pro místní podmínky poskytovatele ZS, ověření funkčnosti (lokání, i předávání dat do NPK), dokumentace.
P.33	Podpora výrobce v režimu min. 8x5, NBD včetně nároku na nejnovější firmware a subskripce (pokud budou vydávány) po dobu min. 5 let.

Tabulka 7: Rozšíření systému pro sběr a analýzu logů v NPK (1.1)

4.4.3.2 Zpracování událostí z analýzy síťového provozu ZZ v NPK (1.2)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

NPK provozuje FortiAnalyzer pro potřeby analýzu síťového provozu. Výstupy z FortiAnalyzer budou zpracovávány v rámci SOC.

#	Požadavek
P.34	Nastavení centrálního zpracování a vyhodnocování událostí z analýzy síťového provozu (z firewalů) na straně ZZ předávány ve FortiAnalyzeru v NPK.
P.35	Předávání dat z dodávaných NGFW na straně poskytovatelů ZS do FortiAnalyzer na straně NPK k vyhodnocení. NGFW poskytovatelů ZS musí být kompatibilní s FortiAnalyzer v rozsahu předávaných dat/událostí.
P.36	Součástí je dodávka, instalace, nastavení, implementace nastavení a pravidel a napojení ZZ na tento systém a související služby.

Tabulka 8: Zpracování událostí z analýzy síťového provozu ZZ v NPK (1.2)

4.4.3.3 Zpracování událostí ze skenování perimetru ZZ v NPK (1.3)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

NPK provozuje technologii FlowMon pro potřeby skenování provozu na perimetru.

Síťový provoz se posílá se do vládního CERT provozovaného ze strany NÚKIB (Národní centrum kybernetické bezpečnosti) k vyhodnocování.

Logy budou předávány do LOGmanageru samostatně, není předmětem této části plnění.

#	Požadavek
P.37	Nastavení centrálního zpracování a vyhodnocování událostí ze skenování perimetru na straně ZZ předávány ve FlowMon v NPK.
P.38	Součástí je dodávka, instalace, nastavení, implementace nastavení a pravidel a napojení ZZ na tento systém a související služby.

Tabulka 9: Zpracování událostí ze skenování perimetru ZZ v NPK (1.3)

4.4.4 Léčebna dlouhodobě nemocných Rybitví (LDN Rybitví)

V této kapitole jsou uvedeny požadavky na dodávky pro: Léčebna dlouhodobě nemocných Rybitví (LDN Rybitví).

4.4.4.1 Nástroje monitorování a bezpečnost počítačových sítí (2.1)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

V rámci zdravotnického zařízení nejsou provozovány nástroje pro monitorování a vyhodnocování síťového provozu, tj. není implementována technologie ani procesy umožňující identifikovat bezpečnostní incidenty a události na úrovni síťového provozu.

Pro identifikaci kybernetických bezpečnostních incidentů/událostí vůči NIS je třeba zahrnout do vyhodnocování dat z provozu síťové komunikační prostředí, které je pro chod NIS nezbytné. Současně je třeba zajistit vyhodnocení/zpracování detekovaných incidentů/událostí, což není na straně ZZ v dostatečném rozsahu možné.

#	Požadavek
P.39	Jedná se o společnou technologii, tj. společné požadavky na dodávku této části jsou uvedeny v kap. 4.4.2 – Společné technologie / 4.4.2.2 – Nástroje monitorování a bezpečnost počítačových sítí.
P.40	Dodávka, implementace, nastavení pro specifické podmínky tohoto ZZ, tj. Léčebna dlouhodobě nemocných Rybitví (LDN Rybitví).
P.41	Zařazení do systému sledování IP provozu sítě CESNET FTAS (https://www.cesnet.cz/sluzby/ftas/) nebo obdobné služby, zajištění vstupního zpracování, klasifikace, filtrace, ukládání záznamů a jejich následné statistické zpracování, vyhledávání a vizualizaci pro správce. *Zřizovací poplatky jsou součástí dodávky, servisní, případně další provozní poplatky jsou součástí servisní smlouvy.*

Tabulka 10: Nástroje monitorování a bezpečnost počítačových sítí (2.1)

4.4.4.2 Nástroje pro ochranu síťového perimetru (2.2)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

Stávající firewally byly pořízeny před několika lety a jejich parametry a funkčnost neodpovídají současným bezpečnostním standardům. Současně je firewall využíván pro provoz celé sítě ZZ, tj. není vyhrazen specificky pro zabezpečení a oddělení perimetru a segmentů ZZ. Je třeba zajistit moderní firewally typu Next Generation Firewall (NGFW) pro sítě využívané pro provoz zabezpečovaného NIS sloužící pro oddělení komunikace a segmentaci sítí zabezpečovaných IS, bezpečnostní a provozní technologie, servery, pracovní

stanice a management a přístup z/do internetu a DMZ, kontrolu síťového provozu pro NIS odděleně od ostatního provozu ZZ.

#	Požadavek
P.42	Je požadována dodávka firewallu/ů typu Next Generation Firewall (NGFW) pro sítě využívané pro provoz zabezpečované IS sloužící pro oddělení komunikace a segmentaci sítí zabezpečovaných IS, bezpečnostní a provozní technologie, servery, pracovní stanice a management a přístup z/do internetu a DMZ, kontrola síťového provozu.
P.43	Základní funkcionality: 1. Firewall, VPN (virtuální privátní sítě IPSec a SSL VPN), Traffic Shaping 2. redundantní řešení v režimu active/active 3. Unified Threat Protection (UTP) 4. řízení bezpečného přístupu mezi vnějšími sítěmi a vnitřní sítí, 5. segmentaci zejména použitím demilitarizovaných zón, 6. podpora NGFW/UTM (AV, IPS, application control), 7. pokročilá hloubková analýza dat na aplikačních (L5-L7) vrstvách ISO modelu, 8. IPS senzor v rámci centrálního Firewall, 9. web filtering, 10. zajištění bezpečného vzdáleného přístupu pro uživatele v souladu s kryptografickými doporučeními (dle § 25 Kryptografické prostředky ZKB) – SSL VPN a IPSec VPN, 11. ověřování VPN uživatelů – integrace s MS Active Directory a podpora pro dvoufaktorovou autentizaci, 12. podpora virtuálních firewallů (kontextů), 13. podpora IPv6, 14. podpora SYSLOG pro zasílání logů, 15. zabezpečený management přes GUI (HTTPS) / CLI (SSH), 16. podpora záložního připojení do internetu, 17. implementace (montáž, instalace, konfigurace, zaškolení, dokumentace), 18. napojení na FortiAnalyzer v NPK pro centrální vyhodnocování událostí, 19. záruka a aktualizace SW, signatur apod. na 5 let.
P.44	Dodávka UTM řešení v provedení dvouuzlového clusteru kompatibilní se současnou technologii Fortinet Fortigate, jehož záznamy se budou přenášet na centrální systém FortiAnalyzer v NPK. Min. celkový požadovaný počet síťových metalických portů Ethernet 1Gb/s je 10. Podpora IPSec VPN, SSL VPN, SD WAN. Součástí dodávky jsou funkce UTM se zakoupenou podporu (maintenance) na 5 let.
P.45	Perimetr infrastruktury požadujeme řešit Next Generation firewallem s funkcionalitami routeru, firewallu, IPS, mailové brány a webové brány. Z důvodů požadavků na vysokou dostupnost požadujeme řešení postavit na dvojici těchto zařízení pracující v režimu „failover“ ActivePassive. V případě výpadku primárního zařízení přebírá automaticky a bezvýpadkově všechny funkcionality sekundární box. Požadované min. parametry pro každý z nich: 1. Provedení: rackmount 2. Rozhraní: 8 x GbE RJ-45, 2 x RJ-45 (konzole a management), 1 x miniUSB, 1 x USB 3.0

#	Požadavek
	3. Podpora PoE: ano, PoE+ (od verze Firepower 6.5 a ASA verze 9.13) 4. Max. propustnost firewallu: 650 Mbps 5. VPN pro min. 50 uživatelů. Součástí dodávky je implementace (montáž, instalace, konfigurace, zaškolení a seznámení s funkcionalitami a obsluhou, dokumentace) Podpora na 5 let typu NBD pro celé dodané řešení této části, oprava v místě instalace zařízení včetně aktualizací všech signatur a SW komponent včetně jejich funkčnosti.
P.46	Dodávka aktivních prvků typu přepínač s podporou 802.1x. Jedná se celkem o 2 ks přepínačů (switchů) které musí plnit následující min. parametry (každý jeden switch): 1. provedení rack mount 2. ethernetový spravovatelný přepínač vrstvy 2 3. min. 24x 10/100/1000Mbs PoE+ TP portů a 4 x 1Gportů SFP 4. minimální propustnost přepínacího subsystému min. 56Gbps 5. možnost zapojení více switchů do jednoho stacku (přepínače se chovají jako jeden z pohledu managementu i připojených zařízení – včetně automatického load balancingu), kapacita propojení 80Gbps – součástí dodávky nejsou požadovány technické prostředky (porty/modul) pro realizaci vlastního stacku, 6. podpora VLAN (min. 1000), 7. software podporující CLI (Telnet/SSH), SNMP management, včetně omezení přístupu na management z definovaných adres a subnetů, 8. bezpečnost – port security a implementace 802.1X, automatické zařazování do VLAN 802.1x – RADIUS server Windows AD, 9. podpora „jumbo“ rámců, 10. detekce protilehlého zařízení (např. CDP nebo LLDP), 11. podpora IPv4 a IPv6, 12. implementace (montáž, instalace, konfigurace, seznámení s funkcionalitami a obsluhou, dokumentace) 13. veškerý potřebný drobný materiál (kabely apod.) Součástí dodávky je implementace (montáž, instalace, konfigurace, zaškolení a seznámení s funkcionalitami a obsluhou, dokumentace) Podpora na 5 let typu NBD pro celé dodané řešení této části, oprava v místě instalace zařízení včetně aktualizací všech signatur a SW komponent včetně jejich funkčnosti.
P.47	Součástí musí být napojení na centrální systém vyhodnocení událostí v NPK, tj. která je na platformě FortiAnalyzer. Důvodem je sjednocení sledování událostí na perimetru sítí jednotlivých ZZ a společné vyhodnocení detekce v rámci NPK (SOC).

Tabulka 11: Nástroje pro ochranu síťového perimetru (2.2)

4.4.4.3 Dodávka Anti-X řešení pro ochranu před škodlivým kódem (2.5)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

V rámci organizace je provozován MS Defender ATP pro 30 licencí stanic z celkového počtu 100 pracovních stanic.

#	Požadavek
P.48	Dodávka centrální antivirové ochrana pro provozní prostředí, komplexní dodávka antivirového řešení pro servery a pracovní stanice, na kterých jsou provozovány zabezpečované IS. Bude sloužit pro ochranu koncových bodů (PC stanic a serverů), které detekuje viry, spyware, adware, podezřelé soubory, chování rootkitů, potencionálně nebezpečné aplikace, ransomware a pokročilý malware. Součástí bude i celková ochrana všech serverů zahrnující ochranu před škodlivým kódem a nastavení všech systémů dle doporučené praxe.
P.49	Základní požadavky: 1. Centrální správa včetně možnosti instalace a kontroly nastavení antivirového systému 2. Napojení na centrální log 3. Notifikace u kritických alertů na správce 4. Reportovací nástroje a příprava základních reportů 5. Vícevrstevná ochrana umožňující zabránit rovněž probíhajícímu malwarovému útoku 6. Detekce zero day hrozeb 7. Ochrana proti zapojení do botnetu 8. Předplatné 5 let (bude zahrnuto do servisních nákladů)
P.50	Technické požadavky: 1. Celé řešení je spravovatelné přes společnou a jednotnou platformu – centrální konzole podporuje správu všech technologií 2. Host Intrusion Prevention (HIPS) - Provádí behaviorální analýzu a zabraňuje síťovým útokům 3. Poskytuje ochranu proti hrozbám typu „zero-day“ a chrání proti útokům „buffer overflow“ zaměřeným na zranitelnosti operačních systémů nebo aplikací 4. Nabízí Data Loss Prevention technologii (DLP) umožňující blokovat dokumenty označené jako důvěrné, aby nemohly být zaslány přes email, webový prohlížeč nebo nahrány na USB disky 5. Filtrování URL adres 6. Umožňuje využití tzv. Security Heartbeat, tj. funkce poskytující sdílenou bezpečnost a informovanost mezi koncovými stanicemi a firewallem, a to v reálném čase 7. Ochrana proti Ransomware – technologie CryptoGuard 8. Pokročilá forma technologie Machine Learning fungující na bázi neuronové sítě 9. Technologie Malicious Traffic Detection monitoruje http provoz a hledá škodlivý provoz (traffic) 10. Zabraňuje neautorizovanému zvyšování oprávnění procesů 11. Technologie Exploit Prevention – zabraňuje zneužívání aplikací (HTML, PowerShell) pomocí internetového browseru 12. Ochraňuje proti krádeži přihlašovacích údajů 13. Grafická analýza původu útoku a jeho průběhu – Root Cause

#	Požadavek
	14. Poskytuje prostředky k včasné identifikaci hrozby a zabránění jejímu dalšímu šíření 15. Izoluje podezřelou či nakaženou stanici od okolní sítě, aby nedocházelo k šíření hrozby 16. Blokuje Exploity 17. Brání hackerům ve využití technik pro eskalaci oprávnění, lateral movement 18. Možnost analýzy souborů prostřednictví cloudu výrobce 19. Investigace hrozeb napříč celou sítí a možnost jednoduchého odstranění hrozeb ze všech stanic spravovaných přes cloudovou konzoli 20. EDR (Endpoint Detection and Response), jde až za hranici endpointů a serverů, a využívá i další zdroje dat jako je firewall, e-mail apod. a poskytuje analýzu útoku – Root Cause 21. Real-Time ochrana před všemi typy PUA a malwaru: a. Viry b. Červy c. trojskými koňmi (backdoor, adware, spyware, rootkit, bootkit, ransomware…) d. Aktivní i pasivní heuristická analýza pro detekci dosud neznámých hrozeb. e. Kontrola RAM paměti pro lepší detekci malwaru využívající silnou obfuskaci a šifrování 22. Možnost jednotlivého zapnutí detekcí: a. potenciálně nechtěných aplikací b. zneužitelných aplikací c. podezřelých aplikací d. Kontrola souborů v průběhu stahování pro snížení celkového času kontroly. e. Skener firmwaru BIOSu a UEFI f. Detekce nespravovaných (rizikových) počítačů komunikujících na síti g. Dynamické skupiny pro možnost definování podmínek, za kterých dojde k automatickému zařazení klienta do požadované skupiny. h. Ochrana proti vypnutí služeb AV řešení i. Možnost přístupu do lokální konzole AV řešení po zadání hesla Administrátora j. Možnost blokace předdefinovaných programů k. Scanování souborů kopírovaných z network folders a USB zařízení l. Ochrana před odinstalací AV m. Napojení na reputační službu n. Možnost rozšíření AV o jiné moduly například o FW modul o. Možnost integrace s Microsoft Defender, kdy MS řeší signaturovou kontrolu a dodaná technologie dodává pokročilé bezpečnostní funkce. Vše je spravováno z jednoho centrálního managementu, viz výše p. Antimalware ochrana pro zařízení s Android q. Možnost rozšíření o on-premise sandbox od stejného výrobce
P.51	Dodávku je možné realizovat rozšířením stávajícího řešení o 70 pracovních stanic. V případě náhrady jinou technologií je součástí dodávka rozšíření o 70 licencí pro pracovní stanice. V případě dodávky jiné technologie musí být předmětem dodávka licencí pro 100 pracovních stanic.
P.52	Součástí je dodávka, instalace, nastavení, implementace nastavení a pravidel a napojení ZZ na tento systém a související služby.

#	Požadavek
P.53	Podpora výrobce v režimu min. 8x5, NBD včetně nároku na nejnovější verze, subskripce (pokud budou vydávány) a signatur po dobu min. 5 let.

Tabulka 12: Dodávka Anti-X řešení pro ochranu před škodlivým kódem (2.5)

4.4.4.4 Nástroje pro sběr logů a významných provozních událostí (2.6)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.54	Jedná se o společnou technologii, tj. společné požadavky na dodávku této části jsou uvedeny v kap. 4.4.2 – Společné technologie / 4.4.2.1 – Nástroje pro sběr logů a významných provozních událostí.
P.55	Dodávka, implementace, nastavení pro specifické podmínky tohoto ZZ, tj. Léčebna dlouhodobě nemocných Rybitví (LDN Rybitví).
P.56	Upgrade stávajících technologií Nagios (www.nagios.org) a Observium (www.observium.org) na aktuální verzi. Součástí je přesun technologií na dodávanou infrastrukturu a zařazení nově dodaných technologií do dohledu v rámci těchto technologií.
P.57	Propojení dodávaných a zabezpečovaných technologií do aktuálně provozovaného systému GrayLOG (graylog.org). Součástí je přesun technologie GrayLOG na dodávanou infrastrukturu.

Tabulka 13: Nástroje pro sběr logů a významných provozních událostí (2.6)

4.4.4.5 Redundantní infrastruktura a nezbytný systémový SW pro záložní DC pro provoz zabezpečovaného IS (2.3, 2.4) a infrastruktura a systémový SW pro provoz bezpečnostních technologií (2.7, 2.8)

V této kapitole jsou uvedeny požadavky na infrastrukturu (HW) a nezbytný systémový SW pro provoz dodávaných technologií.

ZZ nedisponuje redundantní infrastrukturou pro provoz zabezpečovaného NIS a souvisejících technologií. Z uvedeného důvodu není zajištěn provoz v případě výpadku primárních provozních technologií, není zajištěna redundantní infrastruktura pro záložní DC pro provoz zabezpečovaného IS v redundantním/vysoce dostupném režimu a zálohování dat IS, tj. není zajištěna potřebná úroveň dostupnosti informací odpovídající potřebám provozu a poskytování zdravotní péče.

ZZ nedisponuje disponibilní provozní infrastrukturou pro provoz nových bezpečnostních SW technologií. Z důvodu značných kapacitních i výkonnostních nároků nově pořizovaných technologií, primárně pro centrální systém evidence a vyhodnocení logů včetně systému pro detekci narušení bezpečnosti, je třeba zajistit provozní infrastrukturu.

Provozní infrastruktura pro provoz bezpečnostních SW technologií. Z důvodu značných kapacitních i výkonnostních nároků primárně pro centrální systém evidence a vyhodnocení logů včetně systému pro detekci narušení bezpečnosti, nicméně má sloužit i pro provoz ostatních bezpečnostních opatření (sdílení prostředků infrastruktury).

Všechny komponenty bezpečnostní a redundantní infrastruktury budou provozovány na dedikovaném hardware ve virtuálním prostředí (výjimku mohou tvořit např. firewally, sondy provozu a podobná zařízení, která výrobce dodává pouze s dedikovaným HW). S výjimkou firewallů není nutno řešit infrastrukturu

bezpečnost jako vysoce dostupnou. Všechny licence musejí být součástí dodávky jednotlivých komponent bezpečnosti.

Zadavatel předepisuje technologii tam, kde je nezbytné zajistit provozní prostředí pro stávající NIS a další existující IS a technologie, které je třeba zachovat a nové technologie s nimi musí být kompatibilní. V ostatních případech Zadavatel nepředepisuje technologii, jen principy a požadavky na řešení. Technologie bude navržena dodavatelem v nabídce v rámci veřejné zakázky.

HW a SW infrastrukturu není možné v této dokumentaci dostatečně specifikovat, protože jsou závislé na zvolené technologii v rámci řešení konkrétního uchazeče. Zde jsou stanoveny limitní podmínky, které musí uchazeč splnit, tj. nejen technologické podmínky v DC, technologie využívané zadavatelem, ale i požadavky na min. doby pro ukládání dat (min. 5 let) a v návaznosti na splnění těchto podmínek a potřeb technologie, uchazeč navrhne a dodá vhodnou HW a SW infrastrukturu.

#	Požadavek
P.58	Dodávka infrastruktury a běhového prostředí pro následující části dodávky: 1. Virtualizační prostředí pro bezpečnostní technologie a komponenty, které nebudou mít dedikovaný HW (např. nejsou nabízeny a dodávány jako all-in-one). 2. Nástroje monitorování a bezpečnost počítačových sítí (2.1) (kap. 4.4.4.1) 3. Nástroje pro ochranu síťového perimetru (2.2) (kap. 4.4.4.2) 4. Dodávka Anti-X řešení pro ochranu před škodlivým kódem (2.5) (kap. 4.4.4.3) 5. Nástroje pro sběr logů a významných provozních událostí (2.6) (4.4.4.4) 6. Redundantní infrastruktura a nezbytný systémový SW pro záložní DC pro provoz zabezpečovaného IS (2.3, 2.4) Pokud jsou v kapitolách k technologiím odkazovaných v tomto požadavku uvedeny požadavky na výkon, kapacitu, případně jiné parametry, musí HW a systémový SW dodávaný dle této kapitoly plnit podmínky uvedené technologie. Následující požadavky na infrastrukturu (HW) a systémový SW pro běh dodávaného SW jsou minimální, tj. pokud mají dodávky dodavatele nároky vyšší, navrhne dodavatel odpovídající řešení a v nabídce jej popíše.
P.59	Pokud není HW součástí Nástroje pro sběr logů a významných provozních událostí (2.6) dle kap. 4.4.4.4, tak je součástí dodávka HW a systémového SW pro Nástroje pro sběr logů a významných provozních událostí (2.6).
P.60	Dodávka virtualizačního serveru pro virtualizaci komponent NIS a bezpečnostních technologií: 1. Instalace do RACK, max. 2U, včetně rackmount sady 2. Min. 2x CPU Intel Xeon 8C (musí se jednat o typ Intel z důvodu kompatibility s NIS). 3. CPU Xeon 8C 4. RAM 128 GB 5. HDD: 5x SSD 960 GB 6. Porty: min. min. 4x USB, z toho min. 2x USB 3.x, VGA, 2x 1GbE, management porty 7. Podpora OS: Microsoft, SUSE, Red Hat, VMware 8. Redundantní nebo sekundární zdroj 9. Zapojení do management prostředí ZZ (XClarity) Podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení.

#	Požadavek
P.61	Součástí dodávky datové úložiště typu NAS pro ukládání dat z bezpečnostních technologií splňující minimálně: 1. Kapacita pro ukládání dat dodávaných bezpečnostních technologií na 5 let provozu, min. 32 TB. 2. Významné parametry: paměť min. 32 GB, RAID6, 64-bit, 2x 1GbE LAN, 1x 10GbE LAN, 1x USB 3.x, AESNI, PCIe, redundantní zdroj a dostatečný výkon pro chod dodávaných systémů. 3. Instalace do RACK, max. 2U, včetně rackmount sady 4. Systém souborů min.: Btrfs, EXT4, EXT3, FAT, NTFS, HFS, exFAT 5. Připojitelné do virtualizace na dodávané a servery. 6. Podpora ukládání streamů z kamer pro min. 10 kamer. Podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení.
P.62	Dodávka a instalace systémového SW – požadujeme dodávku systémového SW pro všechny dodávané systémy. Jedná se o minimálně následující systémový SW: 1. Virtualizace pro dodávané servery. 2. Operační systémy serverů, kde požadujeme dodávku všech licencí potřebných operačních systémů. 3. Databáze pro dodávané systémy, pokud využívají specifickou databázovou technologii. 4. Technologie pro zajištění redundance/vysoké dostupnosti, pokud by nebyly součástí virtualizace, OS nebo DB. V případě, že nabízené řešení vyžaduje další nespecifikovaný systémový SW tak musí být součástí nabídky.
P.63	Pro server dle požadavku P.60 licence VMware v aktuální verzi pro osazené CPU a počet Core. Dodávaný produkt (varianta) musí podporovat minimálně vysokou dostupnost (HA), živou migraci virtuálního stroje, živou migraci úložiště (virtuálního disku) a akcelerovanou grafiku pro virtuální stroj a kompatibilní se stávajícím řešením. SW plugin či licence, pro zpřístupnění HW dohledu z prostředí VMware vCenter.
P.64	Dodávka stejné licence VMware pro existující server, instalace na existující server a propojení virtualizací obou virtuální serverů.
P.65	Licence zálohovacího systému pro zálohování minimálně dodávaných komponent a systémů tak aby byly zálohovány v rámci jednotného systému zálohování (např. Veeam Backup&Replication, s podporou protokolu DD Boost).
P.66	Dodávka operační systémů pro provoz NIS na dodávané virtuální servery, tj. min. 2x MS Windows Standard, včetně CAL.
P.67	Databázový SW (MS SQL) pro DB NIS pro nově vybudované vysoce dostupné prostředí NIS. NIS je provozován na technologii MS SQL Server.
P.68	Dodávka, zapojení, instalace technologií, instalace a zprovoznění dodávaných technologií a prvků na dodaných technologiích na místě včetně aktualizací všech firmware na poslední aktuální a

#	Požadavek
	stabilní verze a zařazení do monitoringu infrastruktury. Součástí dodávky není strukturovaná kabeláž.

Tabulka 14: Redundantní infrastruktura a nezbytný systémový SW pro záložní DC pro provoz zabezpečovaného IS (2.3, 2.4) a infrastruktura a systémový SW pro provoz bezpečnostních technologií (2.7, 2.8)

4.4.5 Odborný léčebný ústav Jevíčko (OLU Jevíčko)

V této kapitole jsou uvedeny požadavky na dodávky pro: Odborný léčebný ústav Jevíčko (OLU Jevíčko).

4.4.5.1 Nástroje pro ochranu síťového perimetru a vnitřní sítě (3.1)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

Stávající firewally byly pořízeny v roce 2018 a jejich parametry a funkčnost neodpovídají současným bezpečnostním standardům. Současně je firewall využíván pro provoz celé sítě ZZ, tj. není vyhrazen specificky pro zabezpečení a oddělení perimetru a segmentů ZZ. Je třeba zajistit moderní firewally typu Next Generation Firewall (NGFW) pro sítě využívané pro provoz zabezpečovaného NIS sloužící pro oddělení komunikace a segmentaci sítí zabezpečovaných IS, bezpečnostní a provozní technologie, servery, pracovní stanice a management a přístup z/do internetu a DMZ, kontrolu síťového provozu pro NIS odděleně od ostatního provozu ZZ. Na stávající firewally je napojeno 24 AP WiFi. Firewall se využívá jako řídící prvek těchto WiFi, tj. případná modernizace musí toto zachovat.

Stávající WiFi pro zaměstnance, která je připojená do sítě je již zastaralá, tj. je zde riziko kompromitace zařízení kybernetickým útokem. Společně s modernizaci FW je třeba vyměnit 6 ks WIFi routerů, aby byla zajištěna bezpečnost vnitřní sítě jako celku.

#	Požadavek
P.69	Je požadována dodávka firewallu/ů typu Next Generation Firewall (NGFW) pro sítě využívané pro provoz zabezpečované IS sloužící pro oddělení komunikace a segmentaci sítí zabezpečovaných IS, bezpečnostní a provozní technologie, servery, pracovní stanice a management a přístup z/do internetu a DMZ, kontrola síťového provozu. Perimetr infrastruktury požadujeme řešit Next Generation firewallem, tato zařízení v sobě kombinují funkcionality routeru, firewallu, IPS, mailové brány a webové brány. Z důvodů požadavků na vysokou dostupnost požadujeme řešení postavit na dvojici těchto zařízení pracující v režimu „failover“ ActivePassive. V případě výpadku primárního zařízení přebírá automaticky a bezvýpadkově všechny funkcionality sekundární box. Součástí musí být napojení na centrální systém vyhodnocení událostí v NPK, tj. která je na platformě FortiAnalyzer. Důvodem je sjednocení sledování událostí na perimetru sítí jednotlivých ZZ a společné vyhodnocení detekce v rámci NPK (SOC). <u>Základní funkcionality:</u> 1. Firewall, VPN (virtuální privátní sítě IPSec a SSL VPN), Traffic Shaping 2. redundantní řešení v režimu active/passive 3. Unified Threat Protection (UTP) 4. řízení bezpečného přístupu mezi vnějšími sítěmi a vnitřní sítí, 5. segmentaci zejména použitím demilitarizovaných zón, 6. podpora NGFW/UTM (AV, IPS, application control), 7. pokročilá hloubková analýza dat na aplikačních (L5-L7) vrstvách ISO modelu,

#	Požadavek
	8. IPS senzor v rámci centrálního Firewall, 9. web filtering, 10. zajištění bezpečného vzdáleného přístupu pro uživatele v souladu s kryptografickými doporučeními (dle § 25 Kryptografické prostředky ZKB) – SSL VPN a IPSec VPN, 11. ověřování VPN uživatelů – integrace s MS Active Directory a podpora pro dvoufaktorovou autentizaci, 12. podpora virtuálních firewallů (kontextů), 13. podpora IPv6, 14. podpora SYSLOG pro zasílání logů, 15. zabezpečený management přes GUI (HTTPS) / CLI (SSH), 16. podpora záložního připojení do internetu, 17. implementace (montáž, instalace, konfigurace, zaškolení, dokumentace), 18. napojení na FortiAnalyzer v NPK pro centrální vyhodnocování událostí, 19. záruka a aktualizace SW, signatur apod. na 5 let. 20. Možnost připojení a řízení všech stávajících AP (nyní 24 ks). Společně s modernizaci FW je třeba vyměnit 6 ks WiFi routerů, aby byla zajištěna bezpečnost vnitřní sítě jako celku (viz následující požadavky).
WiFi	
P.70	Síť WiFi bude řešena na komponentech podnikové třídy a bude řešit komplexně problematiku bezdrátových připojení ve všech relevantních prostorách zdravotnického zařízení.
P.71	Bude umožněno kvalitní připojení z mobilních zařízení (notebooky, tablety, telefony, …) pro personál i pro pacienty souběžně na stejné infrastruktuře s oddělením komunikace personálu a pacientů (budou zcela odděleny datové toky používané zdravotnickým personálem a pacienty).
P.72	Dodávka 1 ks aktivního prvku typu přepínač s podporou 802.1x, který musí plnit následující min. parametry: 1. provedení rack mount 2. ethernetový spravovatelný přepínač vrstvy 2 3. min. 24x 10/100/1000Mbs PoE+ 4. software podporující CLI (Telnet/SSH), SNMP management, včetně omezení přístupu na management z definovaných adres a subnetů, 5. bezpečnost – port security a implementace 802.1X, automatické zařazování do VLAN 802.1x – RADIUS server Windows AD, 6. podpora IPv4 a IPv6, 7. implementace (montáž, instalace, konfigurace, seznámení s funkcionalitami a obsluhou, dokumentace) 8. veškerý potřebný drobný materiál (kabely apod.) 9. Záruka min. na 5 let.
P.73	Dodávka 6x přístupový bod, každý minimálně v následující konfiguraci: 1. Zařízení musí podporovat minimálně WiFi standardy: 802.11b, 802.11g, 802.11a, 802.11n,802.11ac, 802.11ax 2. Zařízení musí být schopno pracovat současně v pásmu: 2,4 GHz a 5 GHz

#	Požadavek
	3. Počet rádií: 3 4. Počet současně připojených uživatelů: 50 5. Zařízení musí v případě standardu 802.11ax podporovat šířku kanálu až 160MHz. 6. Napájení: PoE napájení dle standardu 802.3at 7. Zařízení musí být dodáno s úchytem na stěnu a/nebo strop 8. Zařízení musí být uzamykatelné proti krádeži. 9. Zařízení musí umožnit konfiguraci minimálně 8 SSID na každém z 802.11 rádií 10. Zařízení musí podporovat minimálně bezpečnostní standardy: WPA2-PSK, WPA2-Enterprise s 802.1X autentizací. 11. Zařízení musí podporovat šifrování: AES 12. Zařízení musí podporovat ověřování: PEAP (MSCHAPv2) 13. Zařízení musí podporovat standardy pro rychlý roaming klientů a rozložení zátěže mezi jednotlivými AP infrastruktury: 802.11r, 802.11k a 802.11v 14. Zařízení podporuje principy QoS: WMM, 802.1p a DSCP. 15. Zařízení musí podporovat funkci rozpoznávání tříd klientských aplikací (dle 7. vrstvy ISO/OSI) a identifikaci operačních systémů a hostname klientských zařízení 16. Zařízení musí být schopné omezit šířku pásma pro každé jednotlivé SSID, pro každého z klientů a také dle rozpoznaných tříd aplikací (dle 7. vrstvy ISO/OSI) 17. Zařízení musí umožnit QoS klasifikaci paketů dle rozpoznaných tříd aplikací (dle 7. vrstvy ISO/OSI) pomocí DSCP a 802.1p tagu 18. Zařízení musí podporovat BLE (Bluetooth Low Energy) dle specifikace Bluetooth 4.0 19. Zařízení musí umožňovat spektrální analýzu pro detekci zdrojů rušení (non-WiFi interference) v pásmu 2,4 a 5GHz s možností zobrazení diagramů v reálném čase. Funkce spektrální analýzy nesmí omezit základní funkci AP – poskytování datové konektivity klientským zařízením 20. Zařízení musí umožnit filtrování procházejících uživatelských dat dle cílových IP adres a/nebo UDP/TCP portů 21. Zařízení musí umožnit zakázat komunikaci vybraných klientů, a to až dle rozpoznaných tříd aplikací (dle 7. vrstvy ISO/OSI) a v případě http i dle DNS jména cílového serveru 22. Zařízení musí mít integrovánu funkci detekce a zastavení útoku na bezdrátovou infrastrukturu (wIDS/wIPS). Tato funkce musí být dostupná v reálném čase na všech kanálech (i neobsluhovaných) a nesmí omezit základní funkci AP – poskytování datové konektivity klientským zařízením 23. Zařízení musí podporovat zachytávání klientského provozu s možností odeslání do ethernetového analyzátoru (např. Wireshark) pro vzdálené řešení problémů připojených klientů. 24. Zařízení musí podporovat L3 roaming klientských zařízení mezi různými subnety sítě 25. Zařízení musí umožnit izolaci jednotlivých uživatelských zařízení tak, aby tato zařízení nemohla komunikovat mezi sebou (v rámci SSID) 26. Zařízení musí být v případě nedostupnosti drátové ethernet konektivity schopné jako uplink dynamicky využít jedno ze svých rádií – mesh link přes některé z okolních AP 27. Zařízení musí umožnit spolu s Centrálním systémem řízení a monitorování sítě lokalizaci klientských zařízení v mapě jednotlivých podlaží na základě triangulace dle síly signálu

#	Požadavek
	28. Zařízení musí umožnit spolu s Centrálním systémem řízení a monitorování sítě poskytovat analytika na základě počtu bezdrátových klientů (i nepřipojených), síly jejich signálu a doby, kterou v dosahu zařízení strávily 29. Zařízení musí být schopné odesílat zprávy na vzdálený SYSLOG server 30. Zařízení musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců 31. Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 60 měsíců, a to včetně výměny vadného hardware, všech aktualizací softwaru a firmwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce 32. Zařízení musí být v době prodeje výrobcem plně podporováno a nesmí být pro něj vyhlášeno ukončení prodeje
P.74	Strukturovaná kabeláž min. CAT 7 (požárně odolné a bezhalogenové se sníženou kouřivostí) a lišty 300 m. Součástí dodávky kabeláže je ukončení v AP, v rozvaděčích/switchích. Kabeláže budou vedeny v podhledech v chodbách jednotlivých objektů, případně mezi patry a objekty existujícími prostupy. Prostupy do jednotlivých místností (pokojů, kanceláří) z chodeb k AP umístěných v místnostech jsou součástí dodávky a montáže, včetně zapravení. *Pozn.: Účtovány budou skutečně dodané objemy.*

Tabulka 15: Nástroje pro ochranu síťového perimetru a vnitřní sítě (3.1)

4.4.5.2 Nástroje monitorování a bezpečnost počítačových sítí (3.2)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

V rámci zdravotnického zařízení nejsou provozovány nástroje pro monitorování a vyhodnocování síťového provozu, tj. není implementována technologie ani procesy umožňující identifikovat bezpečnostní incidenty a události na úrovni síťového provozu.

Pro identifikaci kybernetických bezpečnostních incidentů/událostí vůči NIS je třeba zahrnout do vyhodnocování dat z provozu síťové komunikační prostředí, které je pro chod NIS nezbytné. Současně je třeba zajistit vyhodnocení/zpracování detekovaných incidentů/událostí, což není na straně ZZ v dostatečném rozsahu možné.

#	Požadavek
P.75	Jedná se o společnou technologii, tj. společné požadavky na dodávku této části jsou uvedeny v kap. 4.4.2 – Společné technologie / 4.4.2.2 – Nástroje monitorování a bezpečnost počítačových sítí.
P.76	Dodávka, implementace, nastavení pro specifické podmínky tohoto ZZ, tj. Odborný léčebný ústav Jevíčko (OLU Jevíčko).

Tabulka 16: Nástroje monitorování a bezpečnost počítačových sítí (3.2)

4.4.5.3 Dvoufaktorová autentizace administrátorských VPN přístupů (3.3)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

V rámci ZZ není v současné době využívána dvoufaktorová autentizace.

Ověřování identity uživatelů v rámci přístupu k aktivům IS je prostřednictvím přiděleného loginname/password a jejich ověřování vůči doméně MS Windows a systému MS Active Directory.

VPN přístupy využívají login/password, které se ověřuje vůči DB uživatelů na firewallu (samostatná databáze uživatelů). K samostatnému přístupu do systému se již ověřuje druhé heslo vůči doméně MS Windows a systému MS Active Directory.

#	Požadavek
P.77	Pro zabezpečení vyšší úrovně zabezpečení VPN přístupu privilegovaných účtů je požadována implementace dvoufaktorové autentizace takových uživatelů. Privilegované účty: 1. Správci infrastruktury 2. Správci NIS 3. Bezpečnostní správci 4. Vybraní uživatelé (management) Dvoufaktorová autentizace, která má zabránit neautorizovanému přístupu do systému/sítě, je požadována prostřednictvím mobilního zařízení (mobil) bez nutnosti dalšího hardware. Řešení může být realizováno společně s nástroji pro ochranu síťového perimetru a vnitřní sítě, kde je požadována podpora 2FA u požadovaných zařízení.

Tabulka 17: Dvoufaktorová autentizace administrátorských VPN přístupů (3.3)

4.4.5.4 Zálohovací infrastruktura pro záložní DC pro zálohování dat a technologií zabezpečovaného IS – HW (3.4)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

ZZ nedisponuje dostatečnou infrastrukturou pro zálohování dat zabezpečovaného NIS a souvisejících technologií. Z uvedeného důvodu může v případě výpadku primárních provozních technologií dojít ke ztrátě dat zabezpečovaného NIS bez možnost obnovy těchto dat a obnovení provozu v rámci DRP, tj. není zajištěna potřebná úroveň dostupnosti informací odpovídající potřebám provozu a poskytování zdravotní péče.

#	Požadavek
P.78	Dodávka zálohovací infrastruktury pro zálohování NIS a související provozní SW technologie pro záložní DC pro zálohování dat NIS. Bude se jednat o NAS pro ukládání záloh, např. Synology NAS v konfiguraci min. 6x HDD v kapacitě minimálně 6x 16 TB HDD. Systémový SW a zálohovací technologie budou využity v rámci stávajícího provozního prostředí. V rámci sdílení prostředků infrastruktury může být realizováno společně s provozní infrastrukturou pro provoz bezpečnostních technologií (sdílení prostředků infrastruktury).

Tabulka 18: Zálohovací infrastruktura pro záložní DC pro zálohování dat a technologií zabezpečovaného IS – HW (3.4)

4.4.5.5 Nástroje pro sběr logů a významných provozních událostí (3.5)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.79	Jedná se o společnou technologii, tj. společné požadavky na dodávku této části jsou uvedeny v kap. 4.4.2 – Společné technologie / 4.4.2.1 – Nástroje pro sběr logů a významných provozních událostí.
P.80	Dodávka, implementace, nastavení pro specifické podmínky tohoto ZZ, tj. Odborný léčebný ústav Jevíčko (OLU Jevíčko).

Tabulka 19: Nástroje pro sběr logů a významných provozních událostí (3.5)

4.4.5.6 Infrastruktura a systémový SW pro provoz bezpečnostních technologií (3.6, 3.7)

V této kapitole jsou uvedeny požadavky na infrastrukturu (HW) a nezbytný systémový SW pro provoz dodávaných technologií.

ZZ nedisponuje redundantní infrastrukturou pro provoz zabezpečovaného NIS a souvisejících technologií. Z uvedeného důvodu není zajištěn provoz v případě výpadku primárních provozních technologií, není zajištěna redundantní infrastruktura pro záložní DC pro provoz zabezpečovaného IS v redundantním/vysoce dostupném režimu a zálohování dat IS, tj. není zajištěna potřebná úroveň dostupnosti informací odpovídající potřebám provozu a poskytování zdravotní péče.

ZZ nedisponuje disponibilní provozní infrastrukturou pro provoz nových bezpečnostních SW technologií. Z důvodu značných kapacitních i výkonnostních nároků nově pořizovaných technologií, primárně pro centrální systém evidence a vyhodnocení logů včetně systému pro detekci narušení bezpečnosti, je třeba zajistit provozní infrastrukturu.

Provozní infrastruktura pro provoz bezpečnostních SW technologií. Z důvodu značných kapacitních i výkonnostních nároků primárně pro centrální systém evidence a vyhodnocení logů včetně systému pro detekci narušení bezpečnosti, nicméně má sloužit i pro provoz ostatních bezpečnostních opatření (sdílení prostředků infrastruktury).

Všechny komponenty bezpečnostní a redundantní infrastruktury budou provozovány na dedikovaném hardware ve virtuálním prostředí (výjimku mohou tvořit např. firewally, sondy provozu a podobná zařízení, která výrobce dodává pouze s dedikovaným HW). S výjimkou firewallů není nutno řešit infrastrukturu bezpečnost jako vysoce dostupnou. Všechny licence musejí být součástí dodávky jednotlivých komponent bezpečnosti.

Zadavatel předepisuje technologii tam, kde je nezbytné zajistit provozní prostředí pro stávající NIS a další existující IS a technologie, které je třeba zachovat a nové technologie s nimi musí být kompatibilní. V ostatních případech Zadavatel nepředepisuje technologii, jen principy a požadavky na řešení. Technologie bude navržena dodavatelem v nabídce v rámci veřejné zakázky.

HW a SW infrastrukturu není možné v této dokumentaci dostatečně specifikovat, protože jsou závislé na zvolené technologii v rámci řešení konkrétního uchazeče. Zde jsou stanoveny limitní podmínky, které musí uchazeč splnit, tj. nejen technologické podmínky v DC, technologie využívané zadavatelem, ale i požadavky na min. doby pro ukládání dat (min. 5 let) a v návaznosti na splnění těchto podmínek a potřeb technologie, uchazeč navrhne a dodá vhodnou HW a SW infrastrukturu.

#	Požadavek
P.81	Dodávka 2x virtualizačního serveru pro virtualizaci komponent NIS a bezpečnostních technologií: 1. Instalace do RACK, max. 2U, včetně rackmount sady 2. Min. 2x CPU Intel Xeon 8C (musí se jednat o typ Intel z důvodu kompatibility s NIS). 3. CPU Xeon 8C 4. RAM 128 GB 5. HDD: 5x SSD 960 GB 6. Porty: min. min. 4x USB, z toho min. 2x USB 3.x, VGA, 2x 1GbE, management porty 7. Podpora OS: Microsoft, SUSE, Red Hat, VMware 8. Redundantní nebo sekundární zdroj 9. Zapojení do management prostředí ZZ 10. Zapojení v režimu HA, umístění ve dvou lokalitách. Podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení.
P.82	Pro server dle požadavku P.81 licence virtualizace v aktuální verzi pro osazené CPU a počet Core. Dodávaný produkt (varianta) musí podporovat minimálně vysokou dostupnost (HA), živou migraci virtuálního stroje, živou migraci úložiště (virtuálního disku) a akcelerovanou grafiku pro virtuální stroj a kompatibilní se stávajícím řešením. SW plugin či licence, pro zpřístupnění HW dohledu z prostředí VMware vCenter.
P.83	Dodávka operační systémů pro provoz NIS na dodávané virtuální servery, tj. min. 2x MS Windows Standard, včetně 180 ks CAL.
P.84	Dodávka, zapojení, instalace technologií, instalace a zprovoznění dodávaných technologií a prvků na dodaných technologiích na místě včetně aktualizací všech firmware na poslední aktuální a stabilní verze a zařazení do monitoringu infrastruktury. Součástí dodávky není strukturovaná kabeláž.
P.85	Databázový SW (MS SQL) pro DB NIS pro nově vybudované vysoce dostupné prostředí NIS. NIS je provozován na technologii MS SQL Server.
P.86	Pokud provoz systémů a technologií vyžaduje i další licencovaný SW (databáze, operační systém apod.) musí být všechny licence součástí řešení a zahrnuty v ceně.

Tabulka 20: Infrastruktura a systémový SW pro provoz bezpečnostních technologií (3.6, 3.7)

4.4.6 Albertinum, odborný léčebný ústav Žamberk (OLÚ Albertinum Žamberk)

V této kapitole jsou uvedeny požadavky na dodávky pro: Albertinum, odborný léčebný ústav Žamberk (OLÚ Albertinum Žamberk).

4.4.6.1 Nástroje pro ochranu síťového perimetru (4.1)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

V současnosti je pro ochranu rozhraní vnitřní LAN a sítě internet používán cluster sestavený ze dvou zařízení Fortinet FG60F. Klastr je vybaven pokročilými bezpečnostními funkcemi inspekce provozu na aplikační vrstvě, filtrací webových míst, ochranou proti malware apod. Zároveň je zakoupena servisní podpora v režimu 8 hodin každý pracovní den. Licence na pokročilé bezpečnostní funkce i servisní podporu vyprší v dubnu 2026.

#	Požadavek
P.87	Požadujeme dodat prodloužení licence bezpečnostních funkcí a servisní podpory min. do dubna 2030. Pokud v době realizace zakázky výrobce zařízení Fortinet neposkytoval licenční krytí a servisní podporu do stanoveného data, požadujeme dodávku clusteru se dvěma novými ekvivalentními zařízeními s licencí bezpečnostních funkcí a servisní podpory min. na 5 let provozu dle následujícího požadavku.
P.88	Je požadována dodávka firewallu/ů typu Next Generation Firewall (NGFW) pro sítě využívané pro provoz zabezpečované IS sloužící pro oddělení komunikace a segmentaci sítí zabezpečovaných IS, bezpečnostní a provozní technologie, servery, pracovní stanice a management a přístup z/do internetu a DMZ, kontrola síťového provozu. Perimetr infrastruktury požadujeme řešit Next Generation firewallem, tato zařízení v sobě kombinují funkcionality routeru, firewallu, IPS, mailové brány a webové brány. Z důvodů požadavků na vysokou dostupnost požadujeme řešení postavit na dvojici těchto zařízení pracující v režimu „failover“ ActivePassive. V případě výpadku primárního zařízení přebírá automaticky a bezvýpadkově všechny funkcionality sekundární box. Součástí musí být napojení na centrální systém vyhodnocení událostí v NPK, tj. která je na platformě FortiAnalyzer. Důvodem je sjednocení sledování událostí na perimetru sítí jednotlivých ZZ a společné vyhodnocení detekce v rámci NPK (SOC). <u>Základní funkcionality:</u> 1. Firewall, VPN (virtuální privátní sítě IPSec a SSL VPN), Traffic Shaping 2. redundantní řešení v režimu active/passive 3. Unified Threat Protection (UTP) 4. řízení bezpečného přístupu mezi vnějšími sítěmi a vnitřní sítí, 5. segmentaci zejména použitím demilitarizovaných zón, 6. podpora NGFW/UTM (AV, IPS, application control), 7. pokročilá hloubková analýza dat na aplikačních (L5-L7) vrstvách ISO modelu, 8. IPS senzor v rámci centrálního Firewall, 9. web filtering, 10. zajištění bezpečného vzdáleného přístupu pro uživatele v souladu s kryptografickými doporučeními (dle § 25 Kryptografické prostředky ZKB) – SSL VPN a IPSec VPN, 11. ověřování VPN uživatelů – integrace s MS Active Directory a podpora pro dvoufaktorovou autentizaci, 12. podpora virtuálních firewallů (kontextů), 13. podpora IPv6, 14. podpora SYSLOG pro zasílání logů, 15. zabezpečený management přes GUI (HTTPS) / CLI (SSH), 16. podpora záložního připojení do internetu, 17. implementace (montáž, instalace, konfigurace, zaškolení, dokumentace), 18. napojení na FortiAnalyzer v NPK pro centrální vyhodnocování událostí, 19. záruka a aktualizace SW, signatur apod. na 5 let.

Tabulka 21: Nástroje pro ochranu síťového perimetru (4.1)

4.4.6.2 Redundantní infrastruktura a systémový SW pro záložní DC pro provoz zabezpečovaného IS – HW/SW (4.2, 4.3) a Infrastruktura a systémový SW pro provoz bezpečnostních technologií (4.6, 4.7)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

ZZ nedisponuje redundantní infrastrukturou pro provoz zabezpečovaného NIS a souvisejících technologií. Z uvedeného důvodu není plně zajištěn provoz v případě výpadku primárních provozních technologií, není zajištěna vysoká dostupnost NIS, tj. není zajištěna úroveň dostupnosti informací odpovídající potřebám provozu a poskytování zdravotní péče.

V současnosti se jako velkokapacitní zálohovací medium využívá NAS Synology RS2418RP+ osazených 12 ks HDD 5,5 TB s výslednou nominální diskovou kapacitou 40 TB. Tomuto zařízení vypršela záruka 10.1.2024 a již v nedávné minulosti došlo k jeho havárii, která znemožňovala korektní zálohování kritických serverových komponent.

Stávající kritické agendy jsou provozovány na virtuálních serverech nainstalovaných na jednom virtualizačním VMware ESXi hostiteli zn. DELL PE R440 se dvěma CPU Intel Xeon. Tyto virtuální servery jsou zálohovány systémem Veeam Backup & Replication.

Elektronická zdravotnická dokumentace je nyní archivována na specializované deduplikační a archivační úložiště EMC DataDomain 160 s hrubou kapacitou 1,5 TB, které bylo dodáno v roce 2015.

Virtuální infrastrukturní servery (doménové řadiče MS Active Directory, servery pro vzdálený přístup a pro zálohovací systém) jsou rozmístěny na dvou samostatně stojících virtualizačních VMware hostitelích zn. DELL PE T430, každý se 2 CPU Intel Xeon, které jsou již mimo servisní podporu.

Provozní redundantní infrastruktura a systémový SW pro provoz NIS a související provozní SW technologie pro záložní DC pro provoz zabezpečovaného NIS v redundantním/vysoce dostupném režimu a zálohování dat NIS (a obrazové dokumentace z PACS).

Řešením uvedené situace je vytvoření VMware vSphere H-A clusteru se sdíleným datovým úložištěm osazeným redundantními komponentami (řadiče iSCSI, zdroje, NIC, větráky).

Všechny komponenty redundantní infrastruktury budou provozovány na dedikovaném hardware ve virtuálním prostředí a společně s infrastrukturou v primárním DC bude infrastruktura propojena a provozována jako vysoce dostupná.

V záložním DC bude současně dodána infrastruktura pro zálohování NIS (včetně obrazové dokumentace v PACS) a souvisejících technologií (NAS). Zastaralé a výrobcem nepodporované archivační úložiště bude nahrazeno novým kompatibilním s podporou výrobce min. 5 let.

Zadavatel nepředepisuje konkrétní technologii ani technologické komponenty, jen principy a požadavky na řešení. Technologie bude navržena dodavatelem v nabídce v rámci veřejné zakázky. Zde jsou stanoveny limitní podmínky, které musí uchazeč splnit, tj. nejen technologické podmínky v DC, technologie využívané zadavatelem, ale i požadavky na min. doby pro ukládání dat (min. 5 let) a v návaznosti na splnění těchto podmínek a potřeb technologie, uchazeč navrhne a dodá vhodnou HW a SW infrastrukturu.

#	Požadavek
P.89	Dodávka 2 technicky shodných virtualizačních serverů pro serverovou virtualizaci komponent NIS. Každý server musí splňovat následující požadavky: 1. Instalace do standardního serverového stojanu, včetně rackmount sady 2. Min. 2x 16core CPU Intel Xeon 8C nebo AMD EPYC s taktovací frekvencí min 3 GHz (musí se jednat o jeden z uvedených typů z důvodu kompatibility s NIS). 3. RAM 256 GB 4. 2x HDD SAS min 1TB 5. HBA iSCSI min 10Gb/s včetně 6. Porty: min. min. 4x USB, z toho min. 2x USB 3.x, VGA, 2x 1GbE, management porty 7. Podpora OS: Microsoft, SUSE, Red Hat, VMware 8. Redundantní napájecí zdroj 9. Zapojení v režimu HA, umístění ve dvou lokalitách. Podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení.
P.90	Dodávka diskového pole pro NIS a ukládání dat bezpečnostních technologií splňující minimálně: 1. Kapacita pro ukládání dat dodávaných bezpečnostních technologií na 5 let provozu, celková kapacita min. 8 TB v zapojení RAID10, SAS HDD nebo SSD write intensive. 2. Významné parametry: RAID1,5,6,10, redundantní konektivita iSCSI min. 10Gbps, redundantní zdroj a dostatečný výkon pro chod dodávaných systémů. 3. Připojitelné na dodávané a servery. Podpora na 5 let typu 24x7, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení.
P.91	Součástí dodávky datové úložiště typu NAS pro ukládání dat z bezpečnostních technologií splňující minimálně: 1. Kapacita pro ukládání dat dodávaných bezpečnostních technologií na 5 let provozu, min. 10 TB. 2. Významné parametry: paměť min. 32 GB, RAID6, 64-bit, 2x 1GbE LAN, 1x 10GbE LAN, 1x USB 3.x, AESNI, PCIe, redundantní zdroj a dostatečný výkon pro chod dodávaných systémů. 3. Instalace do RACK, max. 2U, včetně rackmount sady 4. Systém souborů min.: Btrfs, EXT4, EXT3, FAT, NTFS, HFS, exFAT 5. Připojitelné do virtualizace na dodávané a servery. 6. Podpora ukládání streamů z kamer pro min. 10 kamer. Podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení.
P.92	Pro servery dle požadavku P.81 licence virtualizace v aktuální verzi pro osazené CPU a počet Core. Dodávaný produkt (varianta) musí podporovat minimálně vysokou dostupnost (HA), živou migraci virtuálního stroje, živou migraci úložiště (virtuálního disku) a akcelerovanou grafiku pro virtuální stroj a kompatibilní se stávajícím řešením. SW plugin či licence, pro zpřístupnění HW dohledu z prostředí VMware vCenter.

#	Požadavek
P.93	Dodávka operační systémů pro provoz NIS na dodávané virtuální servery, tj. min. 2x MS Windows 2022 Datacenter, včetně 200 device CAL.
P.94	Archivační a deduplikační úložiště DELL PowerProtect DD kompatibilní se stávajícím úložištěm EMC DataDomain160. Hrubá kapacita úložiště min. 4TB, licence na DD Boost, a Retention Lock Compliance Edition, servisní podpora na 5 let. Instalaci a zapojení nového úložiště do archivačního systému provede zadavatel ve vlastní režii.
P.95	Dodávka, zapojení, instalace technologií, instalace a zprovoznění dodávaných technologií a prvků na dodaných technologiích na místě včetně aktualizací všech firmware na poslední aktuální a stabilní verze a zařazení do monitoringu infrastruktury. Součástí dodávky není strukturovaná kabeláž. Výjimkou je dodávka archivačního úložiště dle požadavku P.94, jehož instalaci provede zadavatel ve vlastní režii.
P.96	Licence zálohovacího systému pro zálohování minimálně dodávaných komponent a systémů tak aby byly zálohovány v rámci jednotného systému zálohování Veeam Backup&Replication, s podporou protokolu DD Boost.
P.97	Pokud provoz systémů a technologií vyžaduje i další licencovaný SW (databáze, operační systém apod.) musí být všechny licence součástí řešení a zahrnuty v ceně.

Tabulka 22: Redundantní infrastruktura a systémový SW pro záložní DC pro provoz zabezpečovaného IS – HW/SW (4.2, 4.3) a Infrastruktura a systémový SW pro provoz bezpečnostních technologií (4.6, 4.7)

4.4.6.3 Dodávka Anti-X řešení pro ochranu před škodlivým kódem (4.4)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

Stávající ochrana proti škodlivému SW je nasazena jak na servery, tak i na pracovní stanice v základní konfiguraci chránící tyto servery a pracovní stanice. Je vyřešena řádná a pravidelná aktualizace antivirových databází.

Nicméně není vyřešena centrální správa a sběr a vyhodnocení incidentů jedním centrálním systémem, kde by byly incidenty vyhodnoceny a následně mohla být realizována systémová opatření nikoliv jen na jednom ze zařízení, ale v rámci celého segmentu nebo IS.

Uvedená technologie nezajišťuje dostatečnou kontrolu proti škodlivému kódu a jeho vztažení na aktiva NIS (ohrožení uvedeného IS).

#	Požadavek
P.98	Dodávka centrální antivirové ochrany zabezpečovaného NIS, komplexní dodávka antivirového řešení pro servery a pracovní stanice, na kterých jsou provozovány zabezpečované IS. Bude sloužit pro ochranu koncových bodů (PC stanic a serverů), které detekuje viry, spyware, adware, podezřelé soubory, chování rootkitů, potencionálně nebezpečné aplikace, ransomware a pokročilý malware. Součástí bude i celková ochrana všech serverů zahrnující ochranu před škodlivým kódem a nastavení všech systémů dle doporučené praxe. <u>Základní požadavky:</u> 1. Centrální správa včetně možnosti instalace a kontroly nastavení antivirového systému

#	Požadavek
	2. Napojení na centrální log 3. Notifikace u kritických alertů na správce 4. Reportovací nástroje a příprava základních reportů 5. Vícevrstevná ochrana umožňující zabránit rovněž probíhajícímu malwarovému útoku 6. Detekce zero day hrozeb 7. Ochrana proti zapojení do botnetu 8. Předplatné 5 let (bude zahrnuto do servisních nákladů) <u>Technické požadavky:</u> 1. Celé řešení je spravovatelné přes společnou a jednotnou platformu – centrální konzole podporuje správu všech technologií 2. Host Intrusion Prevention (HIPS) - Provádí behaviorální analýzu a zabraňuje síťovým útokům 3. Poskytuje ochranu proti hrozbám typu „zero-day“ a chrání proti útokům „buffer overflow“ zaměřeným na zranitelnosti operačních systémů nebo aplikací 4. Nabízí Data Loss Prevention technologii (DLP) umožňující blokovat dokumenty označené jako důvěrné, aby nemohly být zaslány přes email, webový prohlížeč nebo nahrány na USB disky 5. Filtrování URL adres 6. Umožňuje využití tzv. Security Heartbeat, tj. funkce poskytující sdílenou bezpečnost a informovanost mezi koncovými stanicemi a firewallem, a to v reálném čase 7. Ochrana proti Ransomware – technologie CryptoGuard 8. Pokročilá forma technologie Machine Learning fungující na bázi neuronové sítě 9. Technologie Malicious Traffic Detection monitoruje http provoz a hledá škodlivý traffic 10. Zabraňuje neautorizovanému zvyšování oprávnění procesů 11. Technologie Exploit Prevention – zabraňuje zneužívání aplikací (HTML, PowerShell) pomocí internetového browseru 12. Ochraňuje proti krádeži přihlašovacích údajů 13. Grafická analýza původu útoku a jeho průběhu – Root Cause 14. Poskytuje prostředky k včasné identifikaci hrozby a zabránění jejímu dalšímu šíření 15. Izoluje podezřelou či nakaženou stanici od okolní sítě, aby nedocházelo k šíření hrozby 16. Blokuje Exploity 17. Brání hackerům ve využití technik pro eskalaci oprávnění, lateral movement 18. Možnost analýzy souborů prostřednictví cloudu výrobce 19. Investigace hrozeb napříč celou sítí a možnost jednoduchého odstranění hrozeb ze všech stanic spravovaných přes cloudovou konzoli 20. EDR (Endpoint Detection and Response), jde až za hranici endpointů a serverů, a využívá i další zdroje dat jako je firewall, e-mail apod. a poskytuje analýzu útoku – Root Cause 21. Real-Time ochrana před všemi typy PUA a malwaru: a. Viry b. Červy c. trojskými koňmi (backdoor, adware, spyware, rootkit, bootkit, ransomware…) d. Aktivní i pasivní heuristická analýza pro detekci dosud neznámých hrozeb.

#	Požadavek
	e. Kontrola RAM paměti pro lepší detekci malwaru využívající silnou obfuskaci a šifrování 22. Možnost jednotlivého zapnutí detekcí: a. potenciálně nechtěných aplikací b. zneužitelných aplikací c. podezřelých aplikací d. Kontrola souborů v průběhu stahování pro snížení celkového času kontroly. e. Skener firmwaru BIOSu a UEFI f. Detekce nespravovaných (rizikových) počítačů komunikujících na síti g. Dynamické skupiny pro možnost definování podmínek, za kterých dojde k automatickému zařazení klienta do požadované skupiny. h. Ochrana proti vypnutí služeb AV řešení i. Možnost přístupu do lokální konzole AV řešení po zadání hesla Administrátora j. Možnost blokace předdefinovaných programů k. Scanování souborů kopírovaných z network folders a USB zařízení l. Ochrana před odinstalací AV m. Napojení na reputační službu n. Možnost rozšíření AV o jiné moduly například o FW modul o. Možnost integrace s Microsoft Defender, kdy MS řeší signaturovou kontrolu a dodaná technologie dodává pokročilé bezpečnostní funkce. Vše je spravováno z jednoho centrálního managementu, viz výše p. Antimalware ochrana pro zařízení s Android q. Možnost rozšíření o on-premise sandbox od stejného výrobce

Tabulka 23: Dodávka Anti-X řešení pro ochranu před škodlivým kódem (4.4)

4.4.6.4 Nástroje monitorování a bezpečnost počítačových sítí (4.1)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

V rámci zdravotnického zařízení je provozován nástroj pro monitorování a vyhodnocování (systém pro detekci a vyhodnocování anomálií) síťového provozu. Zařízení je na konci svého životního cyklu a v 02/2025 mu skončí záruka. Pro zachování kontinuity a ochranu investic požadujeme dodávku srovnatelného nebo lepšího zařízení podle dále uvedených požadavků:

#	Požadavek
P.99	Jedná se o společnou technologii, tj. společné požadavky na dodávku této části jsou uvedeny v kap. 4.4.2 – Společné technologie / 4.4.2.2 – Nástroje monitorování a bezpečnost počítačových sítí.
P.100	Dodávka, implementace, nastavení pro specifické podmínky tohoto ZZ, tj. Albertinum, odborný léčebný ústav Žamberk (OLÚ Albertinum Žamberk).

Tabulka 24: Nástroje monitorování a bezpečnost počítačových sítí (4.1)

4.4.6.5 Nástroje pro sběr logů a významných provozních událostí (4.5)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.101	Jedná se o společnou technologii, tj. společné požadavky na dodávku této části jsou uvedeny v kap. 4.4.2 – Společné technologie / 4.4.2.1 – Nástroje pro sběr logů a významných provozních událostí.
P.102	Dodávka, implementace, nastavení pro specifické podmínky tohoto ZZ, tj. Albertinum, odborný léčebný ústav Žamberk (OLÚ Albertinum Žamberk).

Tabulka 25: Nástroje pro sběr logů a významných provozních událostí (4.5)

4.4.7 Nemocnice následné péče Moravská Třebová (NNP Moravská Třebová)

V této kapitole jsou uvedeny požadavky na dodávky pro: Nemocnice následné péče Moravská Třebová (NNP Moravská Třebová).

4.4.7.1 Nástroje pro ochranu síťového perimetru (5.1)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

Stávající firewally byly pořízeny před několika lety a jejich parametry a funkčnost neodpovídají současným bezpečnostním standardům. Současně je firewall využíván pro provoz celé sítě ZZ, tj. není vyhrazen specificky pro zabezpečení a oddělení perimetru a segmentů ZZ. Je třeba zajistit moderní firewally typu Next Generation Firewall (NGFW) pro sítě využívané pro provoz zabezpečovaného NIS sloužící pro oddělení komunikace a segmentaci sítí zabezpečovaných IS, bezpečnostní a provozní technologie, servery, pracovní stanice a management a přístup z/do internetu a DMZ, kontrolu síťového provozu pro NIS odděleně od ostatního provozu ZZ.

#	Požadavek
P.103	Je požadována dodávka firewallu/ů typu Next Generation Firewall (NGFW) pro sítě využívané pro provoz zabezpečované IS sloužící pro oddělení komunikace a segmentaci sítí zabezpečovaných IS, bezpečnostní a provozní technologie, servery, pracovní stanice a management a přístup z/do internetu a DMZ, kontrola síťového provozu. Perimetr infrastruktury požadujeme řešit Next Generation firewallem, tato zařízení v sobě kombinují funkcionality routeru, firewallu, IPS, mailové brány a webové brány. Z důvodů požadavků na vysokou dostupnost požadujeme řešení postavit na dvojici těchto zařízení pracující v režimu „failover“ ActivePassive. V případě výpadku primárního zařízení přebírá automaticky a bezvýpadkově všechny funkcionality sekundární box. Součástí musí být napojení na centrální systém vyhodnocení událostí v NPK, tj. která je na platformě FortiAnalyzer. Důvodem je sjednocení sledování událostí na perimetru sítí jednotlivých ZZ a společné vyhodnocení detekce v rámci NPK (SOC). <u>Základní funkcionality:</u> 1. Firewall, VPN (virtuální privátní sítě IPSec a SSL VPN), Traffic Shaping 2. redundantní řešení v režimu active/passive 3. Porty minimálně 1x SFP+, 1x 10 GB RJ45 a min. 8x port 1 GB/sec. 4. Unified Threat Protection (UTP)

#	Požadavek
	5. řízení bezpečného přístupu mezi vnějšími sítěmi a vnitřní sítí, 6. segmentaci zejména použitím demilitarizovaných zón, 7. podpora NGFW/UTM (AV, IPS, application control), 8. pokročilá hloubková analýza dat na aplikačních (L5-L7) vrstvách ISO modelu, 9. IPS senzor v rámci centrálního Firewall, 10. web filtering, 11. zajištění bezpečného vzdáleného přístupu pro uživatele v souladu s kryptografickými doporučeními (dle § 25 Kryptografické prostředky ZKB) – SSL VPN a IPSec VPN, 12. ověřování VPN uživatelů – integrace s MS Active Directory a podpora pro dvoufaktorovou autentizaci, 13. podpora virtuálních firewallů (kontextů), 14. podpora IPv6, 15. podpora SYSLOG pro zasílání logů, 16. zabezpečený management přes GUI (HTTPS) / CLI (SSH), 17. podpora záložního připojení do internetu, 18. implementace (montáž, instalace, konfigurace, zaškolení, dokumentace), 19. min. pro 100 uživatelů, 20. napojení na FortiAnalyzer v NPK pro centrální vyhodnocování událostí, 21. záruka a aktualizace SW, signatur apod. na 5 let.

Tabulka 26: Nástroje pro ochranu síťového perimetru (5.1)

4.4.7.2 Nástroje pro identifikaci, autentizaci a řízení oprávnění uživatelů a administrátorů – SW (5.2)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

Ověřování identity uživatelů v rámci přístupu k aktivům IS je prostřednictvím přiděleného loginname/password a jejich ověřování při připojování k PC vůči doméně MS Windows a systému MS Active Directory, tj. využití je omezené jen na přístup do PC, a tedy do sítě ZZ.

V této oblasti byly identifikovány následující nedostatky:

1. V AD nejsou dostatečně definovány doménové účty pro uživatele a zařízení, skupiny uživatelů a politiky pro uživatele a skupiny uživatelů.
2. Není zaveden jednotný způsob ověřování identity uživatelů pro všechny IS a technologie, technologie nejsou napojeny na MS AD, ověřování lokálními účty apod.
3. Není v současné době využívána dvoufaktorová autentizace pro VPN přístupy.
4. Není zavedena integrace na personální systém, která by zajistila automatizované ukončení přístupů v případě ukončení pracovního poměru.

Přístupy do informačního systému nejsou jednotlivým zaměstnancům přidělovány na základě pracovní pozice, všichni zaměstnanci jsou vedeni pod jednou rolí. Přidělení přístupu zaměstnanci do systému nebo aplikace je schvalováno přímým nadřízeným. Přístupová práva jsou poté přidělena zaměstnanci správcem IS. Stejná pravidla jsou nastavena i pro změnu pracovní pozice. Při odchodu zaměstnance jsou, správcem IS na základě informace od přímého nadřízeného, zrušeny přístupy v MS Active Directory. Záznam o odebrání přístupových oprávnění není prováděn. V případě, že správce neobdrží informace o odchodu zaměstnance, nejsou zrušeny přístupy. Řízení přístupů je prováděno pouze zvykově.

Nástrojem pro řízení přístupových oprávnění ZZ disponuje, nicméně část opatření v tomto projektu (oblast c) sekundárně zasahuje do této oblasti, tj. budou provedeny i nezbytné zásahy do tohoto nástroje a rozšíření na celé ZZ včetně zabezpečovaného NIS.

#	Požadavek
P.104	Zavedení MS Active Directory pro identifikaci, autentizaci a řízení oprávnění uživatelů a administrátorů. Součástí bude napojení na NIS (zabezpečovaný systém) a další provozní technologie a řízení oprávnění v MS AD. Součástí jsou licence OS, AD a zapojení v redundantním režimu. Požadováno je tedy zavedení nástrojů pro identifikaci, autentizaci a řízení oprávnění uživatelů a administrátorů pro bezpečnostní technologie a zabezpečované IS. Součástí je vybudování centrálního identity managementu včetně napojení na bezpečnostní technologie a zabezpečované IS a dvoufaktorová autentizace administrátorských VPN přístupů. Autentizace uživatelů NIS bude probíhat prostřednictví MS AD včetně integrace na personální systém a monitoring a reporting. V rámci sjednocení ověřování identity uživatelů v rámci IT a NIS se předpokládá využití stávající domény v rámci Microsoft Active Directory. Nasazení MS Windows Active Directory splňuje následující parametry: 1. definice doménových účtů pro uživatele a zařízení 2. definice skupin uživatelů 3. definice komplexnosti hesla 4. definice politik pro uživatele a skupiny uživatelů 5. služba RADIUS Pro tyto účely požadováno rozšíření stávajícího NIS o možnost autentizace a autorizace v rámci struktury MS Active Directory. NIS bude umožňovat autentizaci a autorizaci uživatelů jak interní, tak také v rámci MS Active Directory. Autorizace uživatelů pro jejich oprávnění pak bude spočívat v příslušnosti k dané skupině uživatelů. Bude vytvořen i interface pro aktualizaci dat uživatelů v AD s personálním systémem (dle aktuálního personálního systému v době definování zadání) tak, aby bylo možné uživatele a případně jejich základní role vytvářet v rámci personálního systému, a hlavně provádět zneplatnění účtů uživatelů, u kterých bude ukončen pracovní poměr. Tím bude zajištěna maximální aktuálnost uživatelských účtů zaměstnanců ZZ.

Tabulka 27: Nástroje pro identifikaci, autentizaci a řízení oprávnění uživatelů a administrátorů – SW (5.2)

4.4.7.3 Nástroje monitorování a bezpečnost počítačových sítí (5.3)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.105	Jedná se o společnou technologii, tj. společné požadavky na dodávku této části jsou uvedeny v kap. 4.4.2 – Společné technologie / 4.4.2.2 – Nástroje monitorování a bezpečnost počítačových sítí.

#	Požadavek
P.106	Dodávka, implementace, nastavení pro specifické podmínky tohoto ZZ, tj. Nemocnice následné péče Moravská Třebová (NNP Moravská Třebová).

Tabulka 28: Nástroje monitorování a bezpečnost počítačových sítí (5.3)

4.4.7.4 Nástroje pro sběr logů a významných provozních událostí (5.4)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.107	Jedná se o společnou technologii, tj. společné požadavky na dodávku této části jsou uvedeny v kap. 4.4.2 – Společné technologie / 4.4.2.1 – Nástroje pro sběr logů a významných provozních událostí.
P.108	Dodávka, implementace, nastavení pro specifické podmínky tohoto ZZ, tj. Nemocnice následné péče Moravská Třebová (NNP Moravská Třebová).

Tabulka 29: Nástroje pro sběr logů a významných provozních událostí (5.4)

4.4.7.5 Redundantní infrastruktura a systémový SW pro záložní DC pro provoz zabezpečovaného IS a bezpečnostních technologií – HW/SW (5.5, 5.6)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

ZZ nedisponuje redundantní infrastrukturou pro provoz zabezpečovaného NIS a souvisejících technologií. Z uvedeného důvodu není zajištěn provoz v případě výpadku primárních provozních technologií, není zajištěna redundantní infrastruktura pro záložní DC pro provoz zabezpečovaného IS v redundantním/vysoce dostupném režimu a zálohování dat IS, tj. není zajištěna potřebná úroveň dostupnosti informací odpovídající potřebám provozu a poskytování zdravotní péče.

Provozní redundantní infrastruktura a systémový SW pro provoz NIS a související provozní SW technologie pro záložní DC pro provoz zabezpečovaného NIS v redundantním/vysoce dostupném režimu a zálohování dat NIS.

Všechny komponenty redundantní infrastruktury budou provozovány na dedikovaném hardware ve virtuálním prostředí a společně s infrastrukturou v primárním DC bude infrastruktura propojena a provozována jako vysoce dostupná.

V záložním DC bude současně dodána infrastruktura pro zálohování NIS a souvisejících technologií.

Zadavatel předepisuje technologii tam, kde je nezbytné zajistit provozní prostředí pro stávající NIS a další existující IS a technologie, které je třeba zachovat a nové technologie s nimi musí být kompatibilní. V ostatních případech Zadavatel nepředepisuje technologii, jen principy a požadavky na řešení. Technologie bude navržena dodavatelem v nabídce v rámci veřejné zakázky.

HW a SW infrastrukturu není možné v této dokumentaci dostatečně specifikovat, protože jsou závislé na zvolené technologii v rámci řešení konkrétního uchazeče. Zde jsou stanoveny limitní podmínky, které musí uchazeč splnit, tj. nejen technologické podmínky v DC, technologie využívané zadavatelem, ale i požadavky na min. doby pro ukládání dat (min. 5 let) a v návaznosti na splnění těchto podmínek a potřeb technologie, uchazeč navrhne a dodá vhodnou HW a SW infrastrukturu.

#	Požadavek
P.109	Dodávka 2x virtualizačního serveru pro virtualizaci komponent NIS a bezpečnostních technologií pro každý server: 1. Instalace do RACK, max. 2U, včetně RackMount sady, 2. Min. 2x CPU 16 Core, 3. RAM 256 GB, 4. HDD: 2x SSD 960 GB, 5. Porty: min. min. 4x USB, z toho min. 2x USB 3.x, VGA, 2x 1GbE, 2x 10 GB SFP+ nebo RJ45, management porty, 6. Podpora OS: Microsoft, SUSE, Red Hat, VMware, 7. Redundantní nebo sekundární zdroj, 8. Zapojení do management prostředí ZZ, 9. Zapojení v režimu HA, umístění ve dvou lokalitách. Podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení.
P.110	Dodávka diskového pole pro NIS a ukládání dat bezpečnostních technologií splňující minimálně: 1. Kapacita pro ukládání dat dodávaných bezpečnostních technologií na 5 let provozu, 2. Max 2U, 3. Možnost rozšíření (další expanzní box), 4. Podpora: snapshot, replikace, tier, 5. 12ks 1.92 TB SSD, 6. 12KS 2.4TB SAS 10K, 7. Významné parametry: RAID6,5,1,0,50, iSCSI min. 10Gbps, min. 2x FC, redundantní zdroj a dostatečný výkon pro chod dodávaných systémů. 8. Připojitelné do virtualizace na dodávané a servery, kompatibilní s VMware. Podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení.
P.111	Součástí dodávky datové úložiště typu NAS pro ukládání dat z bezpečnostních technologií splňující minimálně: 1. Kapacita pro ukládání dat dodávaných bezpečnostních technologií na 5 let provozu, min. 32 TB. 2. Významné parametry: paměť min. 16 GB, RAID6, 64-bit, 2x 1GbE LAN, 1x 10GbE LAN, 1x USB 3.x, AESNI, PCIe, redundantní zdroj a dostatečný výkon pro chod dodávaných systémů. 3. Instalace do RACK, max. 2U, včetně RackMount sady 4. Systém souborů min.: Btrfs, EXT4, EXT3, FAT, NTFS, HFS, exFAT 5. Připojitelné do virtualizace na dodávané a servery (VMware). Podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení.
P.112	Pro server dle požadavku P.109 licence virtualizace v aktuální verzi pro osazené CPU a počet Core. Dodávaný produkt (varianta) musí podporovat minimálně vysokou dostupnost (HA), živou migraci

#	Požadavek
	virtuálního stroje, živou migraci úložiště (virtuálního disku) a akcelerovanou grafiku pro virtuální stroj a být kompatibilní se stávajícím řešením (VMware). SW plugin či licence, pro zpřístupnění HW dohledu z prostředí VMware vCenter. Licence po všechny nody obou dodávaných serverů včetně předplatného na 5 let.
P.113	Dodávka operační systémů pro provoz NIS na dodávané virtuální servery, tj. min. 2x MS Windows Datacenter 2022, včetně licencí 160 User CAL + 15 User RDS CAL.
P.114	Databázový SW (MS SQL) pro DB NIS pro nově vybudované vysoce dostupné prostředí NIS. NIS je provozován na technologii MS SQL Server Standard, tj. dodávka verze min. MS SQL Server 2022 Standard 2core.
P.115	Licence zálohovacího systému pro zálohování minimálně dodávaných komponent a systémů tak aby byly zálohovány v rámci jednotného systému zálohování (např. Veeam Backup&Replication, s podporou protokolu DD Boost).
P.116	Pokud provoz systémů a technologií vyžaduje i další licencovaný SW (databáze, operační systém apod.) musí být všechny licence součástí řešení a zahrnuty v ceně včetně licencí pro uživatele.
P.117	Dodávka, zapojení, instalace technologií, instalace a zprovoznění dodávaných technologií a prvků na dodaných technologiích na místě včetně aktualizací všech firmware na poslední aktuální a stabilní verze a zařazení do monitoringu infrastruktury. Součástí dodávky není strukturovaná kabeláž.

Tabulka 30: Redundantní infrastruktura a systémový SW pro záložní DC pro provoz zabezpečovaného IS a bezpečnostních technologií – HW/SW (5.5, 5.6)

4.4.8 Vysokomýtská nemocnice (NVM)

V této kapitole jsou uvedeny požadavky na dodávky pro: Vysokomýtská nemocnice (NVM).

4.4.8.1 Rozšíření Anti-X řešení pro ochranu před škodlivým kódem (6.1)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

Stávající ochrana proti škodlivému SW je nasazena jak na servery, tak i na pracovní stanice v základní konfiguraci chránící tyto servery a pracovní stanice. Je vyřešena řádná a pravidelná aktualizace antivirových databází. Organizace v současné době používá řešení Sophos Intercept X Advanced, nicméně není aplikováno rozšíření XDR.

Nicméně není vyřešena centrální správa a sběr a vyhodnocení incidentů jedním centrálním systémem, kde by byly incidenty vyhodnoceny a následně mohla být realizována systémová opatření nikoliv jen na jednom ze zařízení, ale v rámci celého segmentu nebo IS.

Uvedená technologie nezajišťuje dostatečnou kontrolu proti škodlivému kódu a jeho vztažení na aktiva NIS (ohrožení uvedeného IS).

#	Požadavek
P.118	Centrální antivirová ochrana zabezpečovaného NIS, rozšíření stávajícího antivirového řešení o nové funkcionality pro servery a pracovní stanice, na kterých jsou provozovány zabezpečované IS. Bude sloužit pro ochranu koncových bodů (PC stanic a serverů), které detekuje viry, spyware, adware, podezřelé soubory, chování rootkitů, potencionálně nebezpečné aplikace, ransomware

#	Požadavek
	a pokročilý malware. Součástí bude i celková ochrana všech serverů zahrnující ochranu před škodlivým kódem a nastavení všech systémů dle doporučené praxe. Bude implementováno rozšíření EDR+XDR pro Anti-X systém. Základní požadavky: 1. Centrální správa včetně možnosti instalace a kontroly nastavení antivirového systému 2. Napojení na centrální log 3. Notifikace u kritických alertů na správce 4. Reportovací nástroje a příprava základních reportů 5. Vícevrstevná ochrana umožňující zabránit rovněž probíhajícímu malwarovému útoku 6. Detekce zero-day hrozeb 7. Ochrana proti zapojení do botnetu 8. Předplatné 5 let (bude zahrnuto do servisních nákladů) Technické požadavky: 1. Celé řešení je spravovatelné přes společnou a jednotnou platformu – centrální konzole podporuje správu všech technologií 2. Host Intrusion Prevention (HIPS) - Provádí behaviorální analýzu a zabraňuje síťovým útokům 3. Poskytuje ochranu proti hrozbám typu „zero-day“ a chrání proti útokům „buffer overflow“ zaměřeným na zranitelnosti operačních systémů nebo aplikací 4. Nabízí Data Loss Prevention technologii (DLP) umožňující blokovat dokumenty označené jako důvěrné, aby nemohly být zaslány přes email, webový prohlížeč nebo nahrány na USB disky 5. Filtrování URL adres 6. Umožňuje využití tzv. Security Heartbeat, tj. funkce poskytující sdílenou bezpečnost a informovanost mezi koncovými stanicemi a firewallem, a to v reálném čase 7. Ochrana proti Ransomware – technologie CryptoGuard 8. Pokročilá forma technologie Machine Learning fungující na bázi neuronové sítě 9. Technologie Malicious Traffic Detection monitoruje http provoz a hledá škodlivý traffic 10. Zabraňuje neautorizovanému zvyšování oprávnění procesů 11. Technologie Exploit Prevention – zabraňuje zneužívání aplikací (HTML, PowerShell) pomocí internetového browseru 12. Ochraňuje proti krádeži přihlašovacích údajů 13. Grafická analýza původu útoku a jeho průběhu – Root Cause 14. Poskytuje prostředky k včasné identifikaci hrozby a zabránění jejímu dalšímu šíření 15. Izoluje podezřelou či nakaženou stanici od okolní sítě, aby nedocházelo k šíření hrozby 16. Blokuje Exploity 17. Brání hackerům ve využití technik pro eskalaci oprávnění, lateral movement 18. Možnost analýzy souborů prostřednictví cloudu výrobce 19. Investigace hrozeb napříč celou sítí a možnost jednoduchého odstranění hrozeb ze všech stanic spravovaných přes cloudovou konzoli 20. EDR (Endpoint Detection and Response), jde až za hranici endpointů a serverů, a využívá i další zdroje dat jako je firewall, e-mail apod. a poskytuje analýzu útoku – Root Cause

#	Požadavek
	21. Real-Time ochrana před všemi typy PUA a malwaru: a. Viry b. Červy c. trojskými koňmi (backdoor, adware, spyware, rootkit, bootkit, ransomware…) d. Aktivní i pasivní heuristická analýza pro detekci dosud neznámých hrozeb. e. Kontrola RAM paměti pro lepší detekci malwaru využívající silnou obfuskaci a šifrování 22. Možnost jednotlivého zapnutí detekcí: a. potenciálně nechtěných aplikací b. zneužitelných aplikací c. podezřelých aplikací d. Kontrola souborů v průběhu stahování pro snížení celkového času kontroly. e. Skener firmwaru BIOSu a UEFI f. Detekce nespravovaných (rizikových) počítačů komunikujících na síti g. Dynamické skupiny pro možnost definování podmínek, za kterých dojde k automatickému zařazení klienta do požadované skupiny. h. Ochrana proti vypnutí služeb AV řešení i. Možnost přístupu do lokální konzole AV řešení po zadání hesla Administrátora j. Možnost blokace předdefinovaných programů k. Scanování souborů kopírovaných z network folders a USB zařízení l. Ochrana před odinstalací AV m. Napojení na reputační službu n. Možnost rozšíření AV o jiné moduly například o FW modul o. Možnost integrace s Microsoft Defender, kdy MS řeší signaturovou kontrolu a dodaná technologie dodává pokročilé bezpečnostní funkce. Vše je spravováno z jednoho centrálního managementu, viz výše p. Antimalware ochrana pro zařízení s Android q. Možnost rozšíření o on-premise sandbox od stejného výrobce

Tabulka 31: Rozšíření Anti-X řešení pro ochranu před škodlivým kódem (6.1)

4.4.8.2 Nástroje pro ochranu síťového perimetru (6.2)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

Stávající firewally Sophos XG135 byly pořízeny před několika lety a jejich parametry a funkčnost neodpovídají současným bezpečnostním standardům. V roce 2025 je ohlášeno ukončení podpory ze strany výrobce. Současně je firewall využíván pro provoz celé sítě ZZ, tj. není vyhrazen specificky pro zabezpečení a oddělení perimetru a segmentů ZZ. Je třeba zajistit moderní firewally typu Next Generation Firewall (NGFW) pro sítě využívané pro provoz zabezpečovaného NIS sloužící pro oddělení komunikace a segmentaci sítí zabezpečovaných IS, bezpečnostní a provozní technologie, servery, pracovní stanice a management a přístup z/do internetu a DMZ, kontrolu síťového provozu pro NIS odděleně od ostatního provozu ZZ.

Preferovaným řešením je výkonnější varianta stejného výrobce s dalšími bezpečnostními funkcemi, jelikož stávající firewally mají návaznost na použité bezpečnostní řešení a technologie (antivirové řešení, WiFi síť).

Stávající řešení není kompatibilní s platformou FortiAnalyzer v NPK, nicméně musí být zajištěna celková kompatibilita s provozním prostředím ZZ.

#	Požadavek
P.119	Je požadována dodávka firewallu/ů typu Next Generation Firewall (NGFW) pro sítě využívané pro provoz zabezpečované IS sloužící pro oddělení komunikace a segmentaci sítí zabezpečovaných IS, bezpečnostní a provozní technologie, servery, pracovní stanice a management a přístup z/do internetu a DMZ, kontrola síťového provozu. Perimetr infrastruktury požadujeme řešit Next Generation firewallem, tato zařízení v sobě kombinují funkcionality routeru, firewallu, IPS, mailové brány a webové brány. Z důvodů požadavků na vysokou dostupnost požadujeme řešení postavit na dvojici těchto zařízení pracující v režimu „failover“ ActivePassive. V případě výpadku primárního zařízení přebírá automaticky a bezvýpadkově všechny funkcionality sekundární box. V případě kompatibilního řešení s platformou FortiAnalyzer v NPK musí být součástí napojení na centrální systém vyhodnocení událostí v NPK, tj. která je na platformě FortiAnalyzer. V případě, že se nebude jednat kompatibilní řešení s platformou FortiAnalyzer v NPK, musí být předávány minimálně logy z nových FW do LOGmanager/SIEM v NPK Důvodem je sjednocení sledování událostí na perimetru sítí jednotlivých ZZ a společné vyhodnocení detekce v rámci NPK (SOC). Základní funkcionality: 1. Firewall, VPN (virtuální privátní sítě IPSec a SSL VPN), Traffic Shaping 2. redundantní řešení v režimu active/passive 3. Unified Threat Protection (UTP) 4. řízení bezpečného přístupu mezi vnějšími sítěmi a vnitřní sítí, 5. segmentaci zejména použitím demilitarizovaných zón, 6. podpora NGFW/UTM (AV, IPS, application control), 7. pokročilá hloubková analýza dat na aplikačních (L5-L7) vrstvách ISO modelu, 8. IPS senzor v rámci centrálního Firewall, 9. web filtering, 10. zajištění bezpečného vzdáleného přístupu pro uživatele v souladu s kryptografickými doporučeními (dle § 25 Kryptografické prostředky ZKB) – SSL VPN a IPSec VPN, 11. ověřování VPN uživatelů – integrace s MS Active Directory a podpora pro dvoufaktorovou autentizaci, 12. podpora virtuálních firewallů (kontextů), 13. podpora IPv6, 14. SandBoxing 15. podpora SYSLOG pro zasílání logů, 16. zabezpečený management přes GUI (HTTPS) / CLI (SSH), 17. podpora záložního připojení do internetu, 18. implementace (montáž, instalace, konfigurace, zaškolení, dokumentace), 19. Předávání událostí do FortiAnalyzer a/nebo do LOGmanager/SIEM v NPK pro centrální vyhodnocování událostí. Varianta bude určena dle kompatibility řešení s platformou FortiAnalyzer a návaznostmi a provozními potřebami vybraného řešení v rámci ZZ. Řešení bude upřesněno v rámci přípravy VZ. 20. záruka a aktualizace SW, signatur apod. na 5 let.

Tabulka 32: Nástroje pro ochranu síťového perimetru (6.2)

4.4.8.3 Nástroje pro segmentaci sítí a řízení přístupu k síti (6.3)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

V rámci infrastruktury ZZ není implementována segmentací sítě. Do systému NIS přistupují uživatelé i z jiných částí sítě v rámci WAN ZZ. Pro bezdrátové připojení uživatelů (WiFi) není implementován přístup do interní sítě na základě implementace 802.1x. Takové zabezpečení není v současné době realizováno ani v rámci drátového připojení v objektech ZZ a nejsou ani všechny lokality vybaveny prvky podporující takovou technologii. Z tohoto důvodu již započala rekonstrukce stávající infrastruktury včetně výměny aktivních prvků.

#	Požadavek
P.120	Požadujeme dodávku (výměnu nevyhovujících) core switchů 2 ks v návaznosti na již provedený upgrade sítě (Cisco – iOS) s min. 24 porty SFP+ včetně modulů 10Gbit (20x fiber, 4x RJ45). Implementace do současné infrastruktury postavené na přístupových switchích Cisco Catalyst 1000 Series.
P.121	Jsou požadovány nástroje pro segmentaci sítí, oddělení podsítí, rozdělení sítí pro zaměstnance, pacienty a návštěvy, sandboxing, Implementace přístupů do LAN sítě (802.1x). Včetně implementace, nastavení a uvedení do provozu. Pro zabezpečení přístupu do LAN/WAN sítě ZZ požadujeme implementaci technologie 802.1x na přístupových switchích centrálních lokalit (2x DC, dodávka 2x switch). Vlastní implementace bude využívat pro ověření zařízení a uživatelů autentizaci v rámci RADIUS serverů Microsoft NPS s integrací do jednotného MS Active Directory. Pro neautorizovaná zařízení a uživatele bude vytvořena v rámci jednotlivých lokalit i GUEST VLAN s definovaně omezeným přístupem do sítě. Správce infrastruktury musí být informován o všech neoprávněných pokusech s maximálním rozsahem informací o takovém pokusu (Datum a čas, MAC adresa, prvek, port apod.). Informace musí být možné získávat online při výskytu nebo reportem za dané časové období. Pro některé lokality bude třeba realizovat i dodávku aktivních prvků typu přepínač s podporou 802.1x v rámci VŘ budou specifikovány počty a vlastnosti takových prvků. Součástí implementace bude i systém logování výskytu jednotlivých zařízení (MAC adres) v rámci WAN ZZ. Systém bude umožňovat jak reporting typu „v kterých lokalitách, prvcích a portech se daná MAC adresa od kdy do kdy byla připojena a jakou IP adresu v rámci WAN ZZ využívala. Reportovací systém bude udržovat databázi výskytu MAC adres a přidělených IP adres jednotlivým MAC adresám s časovou závislostí. Musí být tedy realizována integrace s používanými DHCP servery Microsoft. Reportovací systém musí umožňovat získávat přehled i o připojených zařízeních do aktivních prvků, které nebudou podléhat autentizaci prostřednictvím 802.1x.

Tabulka 33: Nástroje pro segmentaci sítí a řízení přístupu k síti (6.3)

4.4.8.4 Nástroje monitorování a bezpečnost počítačových sítí (6.4)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.122	Jedná se o společnou technologii, tj. společné požadavky na dodávku této části jsou uvedeny v kap. 4.4.2 – Společné technologie / 4.4.2.2 – Nástroje monitorování a bezpečnost počítačových sítí.
P.123	Dodávka, implementace, nastavení pro specifické podmínky tohoto ZZ, tj. Vysokomýtská nemocnice (NVM).

Tabulka 34: Nástroje monitorování a bezpečnost počítačových sítí (6.4)

4.4.8.5 Řízení přístupu uživatelů a administrátorů (6.5)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

V rámci ZZ není v současné době využívána dvoufaktorová autentizace.

Ověřování identity uživatelů v rámci přístupu k aktivům IS je prostřednictvím přiděleného loginname/password a částečně je využíváno jejich ověřování vůči doméně MS Windows a systému MS Active Directory, a to včetně VPN přístupů.

Není zaveden jednotný způsob ověřování identity uživatelů pro všechny IS a technologie (není provedeno napojení všech technologií a NIS na MS AD).

Není zavedena integrace na personální systém, která by zajistila automatizované ukončení přístupů v případě ukončení pracovního poměru.

Z důvodu vyššího zabezpečení požadujeme zavedení technologie ZTNA (Zero Trust Network Access), která umožní významné zvýšení bezpečnosti v našem ekosystému Sophos. Poskytuje jednodušší, lepší a bezpečnější řešení pro připojení uživatelů k důležitým aplikacím a datům.

#	Požadavek
P.124	Je požadováno zavedení dvoufaktorové autentizace jednotlivých uživatelů/zaměstnanců a VPN přístupů s napojením na MS AD. Napojení MS AD na personální systémy s ukončováním přístupů v MS AD a navazujících systémech s ukončením pracovního poměru. Nasazení dvoufaktorové autentizace vůči doméně MS Windows a sytému MS Active Directory v LAN-např. řešení firmy Monet+. Včetně implementace, nastavení a uvedení do provozu. Pro zabezpečení vyšší úrovně zabezpečení VPN přístupu privilegovaných účtů je požadována implementace dvoufaktorové autentizace takových uživatelů. Privilegované účty: 1. Správci infrastruktury 2. Správci NIS 3. Bezpečnostní správci 4. Vybraní uživatelé (management) Dvoufaktorová autentizace, která má zabránit neautorizovanému přístupu do systému/sítě, je požadována prostřednictvím mobilního zařízení (mobil) bez nutnosti dalšího hardware. Bude vytvořen i interface pro aktualizaci dat uživatelů v AD s personálním systémem (dle aktuálního personálního systému v době definování zadání) tak, aby bylo možné uživatele a

#	Požadavek
	případně jejich základní role vytvářet v rámci personálního systému, a hlavně provádět zneplatnění účtů uživatelů, u kterých bude ukončen pracovní poměr. Tím bude zajištěna maximální aktuálnost uživatelských účtů zaměstnanců ZZ. Řešení může být realizováno společně s nástroji pro ochranu síťového perimetru a vnitřní sítě, kde je požadována podpora 2FA u požadovaných zařízení.

Tabulka 35: Řízení přístupu uživatelů a administrátorů (6.5)

4.4.8.6 Zálohovací infrastruktura a SW pro záložní DC pro zálohování dat a technologií zabezpečovaného IS – HW/SW (6.6, 6.7)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

ZZ nedisponuje dostatečnou infrastrukturou pro zálohování dat zabezpečovaného NIS a souvisejících technologií. Z uvedeného důvodu může v případě výpadku primárních provozních technologií dojít ke ztrátě dat zabezpečovaného NIS bez možnost obnovy těchto dat a obnovení provozu v rámci DRP, tj. není zajištěna potřebná úroveň dostupnosti informací odpovídající potřebám provozu a poskytování zdravotní péče.

#	Požadavek
P.125	Zálohovací komponenty infrastruktury budou provozovány na dedikovaném hardware ve virtuálním prostředí, včetně souvisejících SW technologií.
P.126	Dodávka virtualizačního serveru pro zálohování NIS a provoz bezpečnostních technologií: 1. Instalace do RACK, max. 2U, včetně rackmount sady 2. Min. 2x CPU Intel, min. 16 core (musí se jednat o typ Intel z důvodu kompatibility s NIS). 3. RAM 256 GB 4. HDD: 6x SSD 3,8 TB 5. HW Raid controller včetně cache 6. Porty: min. min. 4x USB, z toho min. 2x USB 3.x, VGA, 6x 1GbE, 2x 10 GB SFP+ nebo RJ45, 1x management port 7. Podpora OS: Microsoft, SUSE, Red Hat, VMware 8. Redundantní nebo sekundární napájecí zdroj 9. Zapojení v režimu HA, umístění v primární serverovně 10. Zapojení do management prostředí ZZ (XClarity) Podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení.

#	Požadavek
P.127	Součástí dodávky datové úložiště typu NAS pro ukládání dat z bezpečnostních technologií splňující minimálně: 1. Kapacita pro ukládání dat dodávaných bezpečnostních technologií na 5 let provozu, min. 32 TB. 2. Významné parametry: podpora RAID, 2x 10 GbE LAN, redundantní zdroj a dostatečný výkon pro chod dodávaných systémů. 3. Instalace do RACK, max. 2U, včetně rackmount sady 4. Připojitelné do virtualizace na dodávané a servery. 5. Podpora deduplikace 6. Podpora technologie DD Boost 7. Podpora ukládání streamů z kamer pro min. 10 kamer. Podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení.
P.128	Pro server dle požadavku P.126 licence VMware Standard v aktuální verzi pro osazené CPU a počet Core s podporou min. 5 let. SW plugin či licence, pro zpřístupnění HW dohledu z prostředí VMware vCenter.
P.129	Dodávka operačního systému Microsoft Windows 2022 Datacenter pro provoz záložního serveru vhodný pro zálohovací systém/technologii a záložní provoz NIS.
P.130	Licence zálohovacího systému pro zálohování minimálně pro 30 zálohovaných zařízení, dodávaných komponent a systémů tak aby byly zálohovány v rámci jednotného systému zálohování (např. Veeam Backup&Replication, s podporou protokolu DD Boost) s podporou min. 5 let.
P.131	Pokud provoz systémů a technologií vyžaduje i další licencovaný SW (databáze, operační systém apod.) musí být všechny licence součástí řešení a zahrnuty v ceně.
P.132	V rámci sdílení prostředků infrastruktury může být realizováno společně s provozní infrastrukturou pro provoz bezpečnostních technologií (sdílení prostředků infrastruktury).

Tabulka 36: Zálohovací infrastruktura a SW pro záložní DC pro zálohování dat a technologií zabezpečovaného IS – HW/SW (6.6, 6.7)

4.4.8.7 Nástroje pro sběr logů a významných provozních událostí (6.8)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.133	Jedná se o společnou technologii, tj. společné požadavky na dodávku této části jsou uvedeny v kap. 4.4.2 – Společné technologie / 4.4.2.1 – Nástroje pro sběr logů a významných provozních událostí.
P.134	Dodávka, implementace, nastavení pro specifické podmínky tohoto ZZ, tj. Vysokomýtská nemocnice (NVM).

Tabulka 37: Nástroje pro sběr logů a významných provozních událostí (6.8)

4.4.8.8 Infrastruktura a systémový SW pro provoz bezpečnostních technologií (6.9)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

ZZ nedisponuje disponibilní provozní infrastrukturou pro provoz nových bezpečnostních SW technologií. Z důvodu značných kapacitních i výkonnostních nároků nově pořizovaných technologií, primárně pro centrální systém evidence a vyhodnocení logů včetně systému pro detekci narušení bezpečnosti, je třeba zajistit provozní infrastrukturu.

Provozní infrastruktura pro provoz bezpečnostních SW technologií. Z důvodu značných kapacitních i výkonnostních nároků primárně pro centrální systém evidence a vyhodnocení logů včetně systému pro detekci narušení bezpečnosti, nicméně má sloužit i pro provoz ostatních bezpečnostních opatření (sdílení prostředků infrastruktury).

Všechny komponenty bezpečnostní infrastruktury budou provozovány na dedikovaném hardware ve virtuálním prostředí (výjimku mohou tvořit např. firewally, sondy provozu a podobná zařízení, která výrobce dodává pouze s dedikovaným HW). S výjimkou firewallů není nutno řešit infrastrukturu bezpečnost jako vysoce dostupnou. Všechny licence musejí být součástí dodávky jednotlivých komponent bezpečnosti.

Zadavatel předepisuje technologii tam, kde je nezbytné zajistit provozní prostředí pro stávající NIS a další existující IS a technologie, které je třeba zachovat a nové technologie s nimi musí být kompatibilní. V ostatních případech Zadavatel nepředepisuje technologii, jen principy a požadavky na řešení. Technologie bude navržena dodavatelem v nabídce v rámci veřejné zakázky.

HW a SW infrastrukturu není možné v této dokumentaci dostatečně specifikovat, protože jsou závislé na zvolené technologii v rámci řešení konkrétního uchazeče. Zde jsou stanoveny limitní podmínky, které musí uchazeč splnit, tj. nejen technologické podmínky v DC, technologie využívané zadavatelem, ale i požadavky na min. doby pro ukládání dat (min. 5 let) a v návaznosti na splnění těchto podmínek a potřeb technologie, uchazeč navrhne a dodá vhodnou HW a SW infrastrukturu.

#	Požadavek
P.135	Dodávka virtualizačního serveru pro virtualizaci komponent bezpečnostních technologií: 1. Instalace do RACK, max. 2U, včetně rackmount sady 2. Min. 2x CPU Intel 16 core (musí se jednat o typ Intel z důvodu kompatibility s NIS). 3. RAM 256 GB 4. HDD: 2x SSD 480 GB 5. SAS 12Gbps HBA External Controller 6. Porty: min. 6x 1GbE, 1x management port, 2x 10 GB SFP+ nebo RJ45 7. Podpora OS: Microsoft, SUSE, Red Hat, VMware 8. Redundantní nebo sekundární zdroj 9. HW Raid controller včetně cache 10. Zapojení do management prostředí ZZ (XClarity) Podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení.

#	Požadavek
P.136	Dodávka diskového pole pro provoz bezpečnostních technologií splňující minimálně: 1. Kapacita pro ukládání dat dodávaných bezpečnostních technologií na 5 let provozu, min. 25 TB SSD s možností rozšiřování kapacity. 2. Významné parametry: RAID1,5,6,10, redundantní konektivita iSCSI min. 10Gbps, redundantní zdroj a dostatečný výkon pro chod dodávaných systémů. 3. Připojitelné do virtualizace na dodávané servery. Podpora na 5 let typu 24x7, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení.
P.137	Dodávka záložního zdroje el. energie (UPS) min. 3 kVA. Montáž do RACK max. 2U včetně sad pro montáž, min. 8x zásuvka IEC C13 a min. 2x zásuvka IEC C19, součástí dodávky bude i monitorovací karta.
P.138	Pro server dle požadavku P.135 licence VMware Standard v aktuální verzi pro osazené CPU a počet Core s podporou min. na 5 let. Dodávka další licence VMware Standard v aktuální verzi pro celkový počet 32 CPU Core s podporou 5 let pro zajištění sekundární instalace bezpečnostních technologií. SW plugin či licence, pro zpřístupnění HW dohledu z prostředí VMware vCenter.
P.139	Dodávka operačního systému MS Windows Server 2022 Datacenter pro server dle požadavku kompatibilní s NIS. 1. Dodávka 2x licence MS Windows Server 2022 Datacenter 2. Dodávka 85 ks MS Windows Dev CAL 2022 3. Dodávka 15 ks terminálových licencí MS Windows 2022 4. Dodávka 2 ks licence MS Windows External Connector 2022
P.140	Pokud provoz systémů a technologií vyžaduje i další licencovaný SW (databáze, operační systém apod.) musí být všechny licence součástí řešení a zahrnuty v ceně.
P.141	Dodávka, zapojení, instalace technologií, instalace a zprovoznění dodávaných technologií a prvků na dodaných technologiích na místě včetně aktualizací všech firmware na poslední aktuální a stabilní verze a zařazení do monitoringu infrastruktury. Součástí dodávky není strukturovaná kabeláž.

Tabulka 38: Infrastruktura a systémový SW pro provoz bezpečnostních technologií (6.9)

4.4.9 Rehabilitační ústav Brandýs nad Orlicí (RÚ BnO)

V této kapitole jsou uvedeny požadavky na dodávky pro: Rehabilitační ústav Brandýs nad Orlicí (RÚ BnO).

4.4.9.1 Nástroje pro ochranu síťového perimetru (7.1)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

Stávající firewally byly pořízeny před několika lety a jejich parametry a funkčnost neodpovídají současným bezpečnostním standardům. Současně je firewall využíván pro provoz celé sítě ZZ, tj. není vyhrazen specificky pro zabezpečení a oddělení perimetru a segmentů ZZ. Je třeba zajistit moderní firewally typu Next Generation Firewall (NGFW) pro sítě využívané pro provoz zabezpečovaného NIS sloužící pro oddělení komunikace a segmentaci sítí zabezpečovaných IS, bezpečnostní a provozní technologie, servery, pracovní

stanice a management a přístup z/do internetu a DMZ, kontrolu síťového provozu pro NIS odděleně od ostatního provozu ZZ a mezi dalšími segmenty stě ZZ.

#	Požadavek
P.142	Je požadována dodávka firewallu/ů typu Next Generation Firewall (NGFW) pro sítě využívané pro provoz zabezpečované IS sloužící pro oddělení komunikace a segmentaci sítí zabezpečovaných IS, bezpečnostní a provozní technologie, servery, pracovní stanice a management a přístup z/do internetu a DMZ, kontrola síťového provozu. Perimetr infrastruktury požadujeme řešit Next Generation firewallem, tato zařízení v sobě kombinují funkcionality routeru, firewallu, IPS, mailové brány a webové brány. Z důvodů požadavků na vysokou dostupnost požadujeme řešení postavit na dvojici těchto zařízení pracující v režimu „failover“ Active/Passive. V případě výpadku primárního zařízení přebírá automaticky a bezvýpadkově všechny funkcionality sekundární box. Řešení bude propojeno se stávajícím routerem, společně budou řešeny podsítě ZZ a záložní připojení k internetu. Součástí musí být napojení na centrální systém vyhodnocení událostí v NPK, tj. která je na platformě FortiAnalyzer. Důvodem je sjednocení sledování událostí na perimetru sítí jednotlivých ZZ a společné vyhodnocení detekce v rámci NPK (SOC). <u>Základní funkcionality:</u> 1. Firewall, VPN (virtuální privátní sítě IPSec a SSL VPN), Traffic Shaping 2. redundantní řešení v režimu active/passive 3. Unified Threat Protection (UTP) 4. řízení bezpečného přístupu mezi vnějšími sítěmi a vnitřní sítí, 5. segmentaci zejména použitím demilitarizovaných zón, 6. podpora NGFW/UTM (AV, IPS, application control), 7. pokročilá hloubková analýza dat na aplikačních (L5-L7) vrstvách ISO modelu, 8. IPS senzor v rámci centrálního Firewall, 9. web filtering, 10. zajištění bezpečného vzdáleného přístupu pro uživatele v souladu s kryptografickými doporučeními (dle § 25 Kryptografické prostředky ZKB) – SSL VPN a IPSec VPN, 11. ověřování VPN uživatelů – integrace s MS Active Directory a podpora pro dvoufaktorovou autentizaci, 12. podpora virtuálních firewallů (kontextů), 13. podpora IPv6, 14. podpora SYSLOG pro zasílání logů, 15. zabezpečený management přes GUI (HTTPS) / CLI (SSH), 16. podpora záložního připojení do internetu, 17. implementace (montáž, instalace, konfigurace, zaškolení, dokumentace), 18. napojení na FortiAnalyzer v NPK pro centrální vyhodnocování událostí, 19. záruka a aktualizace SW, signatur apod. na 5 let.

Tabulka 39: Nástroje pro ochranu síťového perimetru (7.1)

4.4.9.2 Nástroje monitorování a bezpečnost počítačových sítí (7.2)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.143	Jedná se o společnou technologii, tj. společné požadavky na dodávku této části jsou uvedeny v kap. 4.4.2 – Společné technologie / 4.4.2.2 – Nástroje monitorování a bezpečnost počítačových sítí.
P.144	Dodávka, implementace, nastavení pro specifické podmínky tohoto ZZ, tj. Rehabilitační ústav Brandýs nad Orlicí (RÚ BnO).

Tabulka 40: Nástroje monitorování a bezpečnost počítačových sítí (7.2)

4.4.9.3 Redundantní infrastruktura a systémový SW pro záložní DC pro provoz zabezpečovaného IS – HW/SW (7.3, 7.4) a Infrastruktura a systémový SW pro provoz bezpečnostních technologií (7.6)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

ZZ nedisponuje redundantní infrastrukturou pro provoz zabezpečovaného NIS a souvisejících technologií. Z uvedeného důvodu není zajištěn provoz v případě výpadku primárních provozních technologií, není zajištěna redundantní infrastruktura pro záložní DC pro provoz zabezpečovaného IS v redundantním/vysoce dostupném režimu a zálohování dat IS, tj. není zajištěna potřebná úroveň dostupnosti informací odpovídající potřebám provozu a poskytování zdravotní péče.

Zadavatel předepisuje technologii tam, kde je nezbytné zajistit provozní prostředí pro stávající NIS a další existující IS a technologie, které je třeba zachovat a nové technologie s nimi musí být kompatibilní. V ostatních případech Zadavatel nepředepisuje technologii, jen principy a požadavky na řešení. Technologie bude navržena dodavatelem v nabídce v rámci veřejné zakázky.

HW a SW infrastrukturu není možné v této dokumentaci dostatečně specifikovat, protože jsou závislé na zvolené technologii v rámci řešení konkrétního uchazeče. Zde jsou stanoveny limitní podmínky, které musí uchazeč splnit, tj. nejen technologické podmínky v DC, technologie využívané zadavatelem, ale i požadavky na min. doby pro ukládání dat (min. 5 let) a v návaznosti na splnění těchto podmínek a potřeb technologie, uchazeč navrhne a dodá vhodnou HW a SW infrastrukturu.

#	Požadavek
P.145	Dodávka 2x virtualizačního serveru pro virtualizaci komponent NIS a bezpečnostních technologií: 1. Instalace do RACK, max. 2U, včetně rackmount sady 2. Min. 1x CPU Intel 32 Core (musí se jednat o typ Intel z důvodu kompatibility s NIS). 3. CPU Xeon 8C 4. RAM 256 GB 5. HDD: 5x SSD 960 GB 6. Porty: min. min. 4x USB, z toho min. 2x USB 3.x, VGA, 2x 1GbE, 2x 10GB SFP+ nebo RJ45, management porty 7. Podpora OS: Microsoft, SUSE, Red Hat, VMware 8. Redundantní nebo sekundární zdroj 9. Zapojení do management prostředí ZZ 10. Zapojení v režimu HA, umístění ve dvou lokalitách. Podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení.
P.146	Dodávka diskového pole pro NIS a ukládání dat bezpečnostních technologií splňující minimálně: 4. Kapacita pro ukládání dat dodávaných bezpečnostních technologií na 5 let provozu, min. 16 TB. 5. Významné parametry: RAID6, iSCSI min. 10Gbps, redundantní zdroj a dostatečný výkon pro chod dodávaných systémů. 6. Připojitelné do virtualizace na dodávané a servery. Podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení.
P.147	Součástí dodávky datové úložiště typu NAS pro ukládání dat z bezpečnostních technologií splňující minimálně: 1. Kapacita pro ukládání dat dodávaných bezpečnostních technologií na 5 let provozu, min. 32 TB. 2. Významné parametry: paměť min. 32 GB, RAID6, 64-bit, 2x 1GbE LAN, 1x 10GbE LAN, 1x USB 3.x, AESNI, PCIe, redundantní zdroj a dostatečný výkon pro chod dodávaných systémů. 3. Instalace do RACK, max. 2U, včetně rackmount sady 4. Systém souborů min.: Btrfs, EXT4, EXT3, FAT, NTFS, HFS, exFAT 5. Připojitelné do virtualizace na dodávané a servery. 6. Podpora ukládání streamů z kamer pro min. 10 kamer. Podpora na 5 let typu NBD, oprava v místě instalace zařízení, servis je poskytován přímo výrobcem zařízení.
P.148	Pro server dle požadavku P.145 licence virtualizace v aktuální verzi pro osazené CPU a počet Core. Dodávaný produkt (varianta) musí podporovat minimálně vysokou dostupnost (HA), živou migraci virtuálního stroje, živou migraci úložiště (virtuálního disku) a akcelerovanou grafiku pro virtuální stroj a kompatibilní se stávajícím řešením. SW plugin či licence, pro zpřístupnění HW dohledu z prostředí MS Hyper-V.

#	Požadavek
P.149	Dodávka operační systémů pro provoz NIS na dodávané virtuální servery, tj. min. 2x MS Windows Datacenter, včetně 110 ks CAL.
P.150	Technologie pro zajištění redundance/vysoké dostupnosti, pokud by nebyly součástí virtualizace, OS nebo DB.
P.151	Licence zálohovacího systému pro zálohování minimálně dodávaných komponent a systémů tak aby byly zálohovány v rámci jednotného systému zálohování (např. Veeam Backup&Replication, s podporou protokolu DD Boost, Acronis).
P.152	Pokud provoz systémů a technologií vyžaduje i další licencovaný SW (databáze, operační systém apod.) musí být všechny licence součástí řešení a zahrnuty v ceně.
P.153	Dodávka, zapojení, instalace technologií, instalace a zprovoznění dodávaných technologií a prvků na dodaných technologiích na místě včetně aktualizací všech firmware na poslední aktuální a stabilní verze a zařazení do monitoringu infrastruktury. Součástí dodávky není strukturovaná kabeláž.

Tabulka 41: Redundantní infrastruktura a systémový SW pro záložní DC pro provoz zabezpečovaného IS – HW/SW (7.3, 7.4) a Infrastruktura a systémový SW pro provoz bezpečnostních technologií (7.6)

4.4.9.4 Nástroje pro sběr logů a významných provozních událostí (7.5)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.154	Jedná se o společnou technologii, tj. společné požadavky na dodávku této části jsou uvedeny v kap. 4.4.2 – Společné technologie / 4.4.2.1 – Nástroje pro sběr logů a významných provozních událostí.
P.155	Dodávka, implementace, nastavení pro specifické podmínky tohoto ZZ, tj. Rehabilitační ústav Brandýs nad Orlicí (RÚ BnO).

Tabulka 42: Nástroje pro sběr logů a významných provozních událostí (7.5)

4.4.10 Ostatní systémy a technologie

V této kapitole jsou uvedeny požadavky na ostatní dodávky.

4.4.10.1 Nástroje pro penetrační testy a penetrační testy (8.1)

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.156	Je požadována dodávka nástroje/nástrojů pro periodické testování bezpečnostních zranitelností interních systémů i systémů, které komunikují s externími subjekty i jako součást penetračních testů.
P.157	Minimální rozsah: externí testy, interní testy a testy zranitelností operačních systémů, databází a informačních systémů (aplikací).

#	Požadavek
	Jedná se minimálně o: 1. Host Discovery – vyhledávání aktivních strojů; 2. Port Scanning – skenování portů; 3. Service Discovery – vyhledání běžící služby; 4. Web Applications – skenování webových aplikací;
P.158	Je požadováno, aby nástroj/nástroje umožňoval: 1. Vzdálené privilegované a neprivilegované skeny 2. Neomezené množství koncových IP adres 3. Pravidelné aktualizace signatur/detekčních metod (cca 1x týdně)
P.159	Předmětem dodávky není periodické provádění testů zranitelností (nad rámec testů v rámci vedlejších aktivit), ale zajištění nástrojů pro provádění a vyhodnocování uvedených testů.
P.160	S ohledem na vysokou citlivost zpracovávaných dat musí být dodaný nástroj možné kompletně instalovat na server/počítač umístěný v lokální síti, která je pod správou Zadavatele. Výstupy z testů/skenů musí být rovněž zpracovávány lokálně, bez zasílání do cloudu. Dodaný nástroj musí umožňovat ovládání s pomocí webového GUI.
P.161	Instalaci skeneru musí být možné realizovat na prvky s operačními systémy Microsoft Windows 10 a vyšší, Microsoft Windows Server 2012 a vyšší, macOS i Linux. Součástí dodávky nebude HW, OS ani další aplikační vybavení nutné pro provoz nástroje. Předpokládá se instalaci na prostředky Zadavatele (virtuální server nebo testovací PC/notebook).
P.162	Dodané řešení musí podporovat realizaci vzdálených bezagentských privilegovaných i neprivilegovaných skenů neomezeného počtu zařízení/IP adres a musí být schopné realizovat bezpečnostní skeny webových aplikací.
P.163	Řešení musí být schopné identifikovat chybějící záplaty/zranitelné služby a aplikace běžící na skenovaných systémech.
P.164	Součástí dodávky bude licence relevantního nástroje s podporou a funkčností po dobu 5 let, instalace a aktivace jednoho skeneru v prostředí Zadavatele a úvodní zaškolení administrátorů a uživatelů.
P.165	Provedení penetračních testů a testů zranitelnosti: 1. Provedení penetračních testů a testů zranitelnosti pro zabezpečované IS (informační systémy a technologie jsou popsány v kap. 7.2 – Informační systémy k zabezpečení). 2. Pro zabezpečované systémy budou provedeny závěrečné testy zranitelnosti z externí sítě. V zájmu ověření korektního fungování zabezpečení komunikační sítě a zajištění vysoké úrovně bezpečnosti provozovaných aplikací je požadováno provedení jednorázových penetračních testů.
P.166	Závěrečné testy zranitelnosti budou provedeny z externí sítě na zabezpečované. Jedná se tedy o testy zranitelnosti realizované přes bezpečnostní prvky – perimetry (FireWall). Tyto testy musí obsahovat min.: 1. Host Discovery – vyhledávání aktivních strojů;

#	Požadavek
	2. Port Scanning – skenování portů; 3. Service Discovery – vyhledání běžící služby; 4. Web Applications – skenování webových aplikací; Účelem těchto testů je ověření konfigurace perimetrů a nalezení zranitelností publikovaných služeb/systémů.
P.167	V zájmu ověření a zajištění vysoké úrovně bezpečnosti provozovaných aplikací je požadováno provedení jednorázových penetračních testů. Penetrační testy musí splňovat minimálně: 1. Penetrační testy se budou týkat uvedených aplikací provozovaných zadavatelem a jejich účelem bude identifikovat případné nedostatky v nastavení nasazeného WAF a odhalit případné zranitelnosti ve výše uvedených aplikacích, které jsou jím chráněny, a zajistit tak jejich bezpečnost v rámci plnění požadavků §25 vyhlášky 82/2018 Sb. V souladu s bezpečnostní strategií a dalšími dokumenty zadavatele. 2. Testy budou provedeny jak při využití WAF, tak přímo vůči serveru, který aplikaci poskytuje. Testy budou provedeny jak autentizovanou (s právy běžného uživatele), tak neautentizovanou formou (anonymní přístup). 3. Součástí testů nebude vyhledávání zranitelností v síťové ani jiné infrastruktuře, virtualizačních platformách ani dalším SW vybavení serverů provozujících uvedené aplikace, které s provozem daných aplikací přímo nesouvisí. Před vlastními penetračními testy bude proveden test zranitelností. Testy budou realizovány dle aktuální verze OWASP Web Security Testing Guide (WSTG) a v souladu s metodikou OSSTMM a budou primárně zaměřeny na odhalování zranitelností dle platné verze OWASP Top 10. Využito při tom bude automatizovaných nástrojů i manuálního testování.
P.168	Výstupem testů zranitelnosti a penetračních testů musí být: 1. Závěrečná zpráva, která bude obsahovat soupis provedených testů a jejich výsledků, detailní popis odhalených zranitelností, ohodnocení jejich nebezpečnosti včetně konkrétního postupu umožňujícího jejich odstranění. 2. Doporučení řešení odhalených zranitelností – konkrétní postupy umožňující jejich odstranění u oblastí/technologií, které nejsou součástí dodávky. 3. Realizace opatření k odstranění odhalených zranitelností ve formě nastavení a implementace u oblastí, které jsou součástí dodávky.

Tabulka 43: Nástroje pro penetrační testy a penetrační testy (8.1)

4.4.11 Bezpečnostní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.169	Systém bude chránit osobní údaje pacientů a bude v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob (GDPR) v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

#	Požadavek
P.170	Vybavení musí plnit podmínky zákona č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
P.171	Autorizace: Poskytnutí přístupu autentizovaného uživatele k aktivu systému (data, aplikace), odpovídající pracovnímu zařazení uživatele a přidělené roli (rolím) v systému. Systém umožní řídit přístupová oprávnění jednotlivých subjektů jen k údajům, ke kterým mají a mohou mít přístup.
P.172	Zabránění vstupu neautorizovaného subjektu do systému – zamezení možnosti přístupu neoprávněného subjektu.
P.173	Zajištění šifrované komunikace mezi všemi součástmi systému a pracovišti uživatelů, případně zajištění komunikace v odděleném síťovém prostředí.
P.174	Evidence přístupů všech uživatelů do systémů a technologií (logování) včetně časových údajů.
P.175	Veškeré přístupy k datům a aktivita uživatelů v rámci dodávaných systémů a technologií budou logovány tak, aby byly zřejmé přístupy k jednotlivým údajům a zpětná kontrola těchto údajů.
P.176	Veškeré logy budou dostupné pro externí systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí.

Tabulka 44: Bezpečnostní požadavky

4.4.12 Implementační a provozní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.177	Všechny komponenty musí být připraven na provoz 24x7x365 (non-stop).
P.178	Počet uživatelů informačních systémů a technologií se nezmění.
P.179	Předmětem zakázky jsou i veškeré služby související s dodávkou – doprava, instalace, implementace do stávající infrastruktury, konfigurace a zprovoznění komunikace, nastavení datových toků, seznámení s obsluhou a správou systému, testování, bezplatné preventivní prohlídky v rámci poskytování servisních služeb. Veškeré seznámení s obsluhou bude probíhat v prostorách objednatele a v českém jazyce. Součástí nabídkové ceny musí být i veškeré práce či činnosti, které v této zadávací dokumentaci nejsou explicitně uvedeny, ale které musí dodavatel s ohledem na jím nabízený předmět veřejné zakázky a jeho řádnou a úplnou realizaci provést k dosažení objednatelem požadovaného cílového stavu.
P.180	Instalace do prostředí objednatele a jeho ZZ uvedených ve výchozím stavu.
P.181	V rámci implementace musí dodavatel zajistit plnohodnotný provoz dodávaného řešení současně s provozem stávajících systémů a technologií. To vše s minimálním omezením provozu. Dodavatel je povinen přizpůsobit realizaci předmětu zakázky podmínkám objednatele.
P.182	Dodávka OS na servery, včetně instalace do prostředí objednatele, vč. potřebných licencí, pokud se jedná o licencovaný OS.

#	Požadavek
P.183	Všechny dodávané nebo upravované součástí systémů (OS, DB, IS, klientské aplikace) musí logovat svou činnost do logů s možností nastavit úroveň logování pro potřeby diagnostiky.
P.184	Zálohování – dodávaný systém (virtualizace, OS) a DB musí být schopny a připraveny na zálohování systémem objednatele, tj. pro virtualizaci, OS a DB musí existovat agenti umožňující zálohování ze strany objednatele.
P.185	Zajištění administrátorských aplikací, konzolí pro všechny součástí systému (OS, DB, IS, …) pro zajištění konfiguračního managementu systému anebo jeho součástí.
P.186	Dohled – dodávané systémy a technologie musí předávat informace o svém stavu (stavu služeb apod.) na žádosti SNMP GET. Zhotovitel poskytne parametry, podmínky a součinnost při nastavení dohledu dodaného řešení.
P.187	Architektura řešení celého systému musí korespondovat s požadavky na jeho dostupnost, uvedenými v servisní smlouvě.
P.188	Synchronizace času všech zařízení s time serverem nebo zprostředkovaně přes centrální systém.

Tabulka 45: Implementační a provozní požadavky

4.5 POŽADAVKY NA SLUŽBY

4.5.1 Realizace předmětu plnění

Součástí předmětu plnění je zajištění služeb souvisejících s realizací předmětu plnění minimálně v následujícím rozsahu:

1) Objednatel požaduje před zahájením implementačních prací zpracování **Implementační analýzy včetně návrhu řešení** (konkretizace implementačního postupu, přesné konfigurace a instalačního a montážního návrhu řešení z nabídky), která bude zahrnovat informace pro všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění. Implementační analýza včetně návrhu řešení musí být před zahájením prací schválena objednatelem. Implementační analýza včetně návrhu řešení musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu a musí obsahovat minimálně tyto části:
   a) Implementační analýza – zjištění týkající se prostředí objednatele, bude obsahovat alespoň následující:
      i) Seznam technologií, které mají vliv/dopad na dodávku
      ii) Identifikace zdrojů dat využitých pro dodávku
      iii) Evaluace bezpečnosti systému a rizikových faktorů
      iv) Implementační upřesnění specifikace požadavků
      v) Výstupy z analýzy okolí – sběr a analýza informací vztahujících se k dodávce (např. součinnosti apod.)
   b) Detailní popis cílového stavu (instalační a montážní upřesnění návrhu řešení z nabídky)

      Popis bude obsahovat alespoň:
      i) Rozpracování návrhu řešení z nabídky zhotovitele z pohledu instalací a montáže dle informací z implementační analýzy
      ii) Upřesnění rozhraní pro integraci na IS a technologie třetích stran (v případě nutnosti)

iii) Způsob zajištění projektového řízení na straně zhotovitele pro realizaci předmětu plnění (harmonogram, projektový tým, koordinační mechanismy apod.)

iv) Detailní návrh a popis postupu implementace, instalace a montáže předmětu plnění

v) Detailní popis zajištění bezpečnosti systému a informací

Detailní harmonogram projektu včetně uvedení kritických milníků. Kritické milníky jsou termíny dosažení určitých fází projektu, které jsou pro naplnění cílů projektu klíčové. Kritické milníky budou obsahovat minimálně aktivity vedené v kapitole 5 - Harmonogram, s uvedením konkrétních termínů, zhotovitel vhodným způsobem může rozšířit kritické milníky o další aktivity, které mohou být pro projekt klíčové.

vi) Detailní popis navrhovaného seznámení s funkcionalitami, obsluhou dodávaných technologií a budoucím provozem.

2) **Zajištění projektového vedení/řízení** realizace předmětu plnění ze strany zhotovitele a jeho případných subdodavatelů.

3) **Vývoj, implementace a nastavení** informačních a komunikačních technologií odpovídající schválenému návrhu řešení uvedenému v Implementační analýze a příprava pro ověření ze strany objednatele, alespoň v následujícím rozsahu:

a) Vývoj na straně zhotovitele – vývoj jednotlivých systémů, úpravy existujících produktů, jejich parametrizace a nastavení, vývoj a ověřování integračních rozhraní, součinnost se třetími stranami v souvisejících oblastech.

b) Instalace a implementace do prostředí objednatele v testovacím režimu.

c) Interní ověření na straně zhotovitele a příprava podkladů pro ověření na straně objednatele (dokumentace, organizace testování a další).

d) Příprava a naplnění základních dat – z integračních úloh, číselníky, uživatelé a další.

Provedením těchto činností bude zajištěna připravenost pro ověření ze strany objednatele.

4) **Dodávka předmětu plnění**. Součástí dodávky musí být instalace, upgrade a sestavení předmětu zakázky včetně:

a) Instalace, upgrade a zahoření HW na místě,

b) Instalace a nastavení HW a SW budou provedeny kvalifikovanými osobami pro dané typy zařízení

c) Nastavení HW a aplikací

5) **Zajištění instalace všech součástí dodávky** v určených lokalitách a prostorách objednatele.

6) **Zajištění instalace a připojení** k zařízením a technickým prostředkům zajištěným objednatelem.

7) **Realizace pilotního provozu** k ověření funkčnosti systému na menším obejmu dat, s menším počtem uživatelů a na menším počtu zařízení.

8) **Převedení systémů do zkušebního provozu** a plná podpora uživatelů v rámci zkušebního provozu včetně technické podpory. V této etapě budou realizována požadovaná seznámení s funkcionalitami, obsluhou dodávaného zařízení a budoucím provozem.

9) **Zpracování dokumentace skutečného provedení, systémové a provozní dokumentace** – součástí předmětu plnění je zajištění systémové a provozní dokumentace související s realizací předmětu plnění minimálně v následujícím rozsahu:

Název	Popis
Uživatelská dokumentace	Bude popisovat konkrétní funkčnost z pohledu uživatele tak, aby byl uživatel schopen práce s informačním systémem a pochopil význam

Název	Popis
	jednotlivých částí systému a vazeb mezi nimi. V uživatelské příručce bude popisován způsob práce s jednotlivými částmi systému, vazby mezi nimi včetně popisu součástí jednotlivých částí systému. K usnadnění práce bude sloužit popis jednotlivých obrazovek, ovládacích prvků na obrazovkách a jejich významů, který bude uveden v rámci uživatelské dokumentace.
Dokumentace skutečného provedení a systémová/provozní dokumentace	Obsahuje popis informačního systému (rozhraní a služby) včetně popisu správy informačního systému, definování uživatelů, jejich oprávnění a povinností a detailní popis údržby systému.
Bezpečnostní dokumentace	Účelem bezpečnostní dokumentace je definovat závazná pravidla pro zajištění informační bezpečnosti včetně stanovení bezpečnostních opatření. Součástí této dokumentace bude uveden seznam, který bude obsahovat seznam všech externích zdrojů, ke kterým se jednotlivé servery (součásti systému) připojují, včetně uvedení síťových protokolů, pomocí kterých se s daným externím zdrojem komunikuje. V případě, že na servery (součásti systému) existuje vzdálený přístup, musí být tento přístup jasně specifikován (vzdálené zařízení, síťový protokol) a popsán zdůvodnění takovéhoto přístupu (dohled, správa DB atd.)
Disaster & Recovery Plan	Plán řešení situací v případě výpadků a obnovy funkčnosti systému. Součástí je plán a způsob provádění zálohy a případného způsobu obnovy a obnovy funkčnosti i v případě jiných technických výpadků. Dokument bude vytvářen v součinnosti s objednatelem.
Projektová dokumentace	Smluvní dokumentace, harmonogram realizace projektu, analýzy a prováděcí projekty, zápisy z jednání, protokoly (předávací, akceptační)

Tabulka 46: Dokumentace – požadavky na zpracování

Dokumentace bude dodána v relevantním rozsahu na všechna místa plnění projektu.

Dokumentace bude v souladu se zákonem č. 365/2000 Sb. o informačních systémech veřejné správy a prováděcích právních předpisů, v platném znění.

Dokumenty budou zpracovávány v následujících programech elektronicky a uloženy v následujících formátech:

- MS Office 2016 (MS Word 2016, MS Excel 2016, MS PowerPoint 2016)
- MS Project 2016
- WinZip (formát .zip)
- Portable Document Format (formát .pdf).

Preferovaná forma předávaných dokumentů, které nebudou vyžadovat podpisy konkrétních osob je elektronicky, a to na elektronických nosičích (CD, DVD, flash disk atp.) nebo online úložištích (Sharepoint apod.). K předávání a k archivaci souborů se používají média s možností pouze zápisu, nikoliv přepisovatelná.

Veškerá dokumentace bude podléhat schvalování (akceptaci) při převzetí ze strany objednatele.

Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána ve 2x kopiích v elektronické formě ve standartních formátech (MS Office a PDF) používaných objednatelem. Listinná forma není požadována

10) **Provedení akceptačních testů.** Zhotovitel je povinen kompletně připravit podklady pro akceptaci dodaného řešení. Součástí akceptace bude akceptační protokol a kompletní předávací dokumentace.
11) **Uvedení systému do produkčního provozu**, zajištění potřebných nastavení a přístupů pro všechny pracovníky objednatele, minimalizace dopadů na provoz objednatele při přechodu a zvýšená podpora bezprostředně po přechodu do produkčního provozu.
12) Zhotovitel dle svého uvážení doplní v nabídce další služby, které jsou dle jeho názoru nezbytné pro úspěšnou realizaci zakázky.
13) Veškeré náklady na zajištění služeb souvisejících s realizací předmětu plnění musí být zahrnuty v ceně odpovídající části předmětu dodávky.

4.5.2 Seznámení s funkcionalitami, obsluhou dodávaných technologií

V této kapitole jsou uvedeny požadavky na seznámení s funkcionalitami, obsluhou dodávaných technologií a jejich budoucím provozem:

1) Zhotovitel proškolí pracovníky objednatele se všemi typy dodaných zařízení a aplikací a problematikou jejich užití, provozu a obsluhy. Zhotovitel se zavazuje poskytnout informace minimálně k následujícím tématům v dostatečném detailu pro porozumění činnosti zařízení a způsobu provozu:
    a. Základní produktové seznámení s jednotlivými dílčími technologickými celky.
    b. Celkové schéma součinnosti jednotlivých zařízení a jejich návaznosti.
    c. Obsluha jednotlivých dílčích modulů, aplikací a technologických celků
    d. Použitá nastavení zařízení, detailnější rozbor použitých konfigurací.
    e. Základní kroky správy, diagnostiky a elementární postupy pro řešení problémů.
2) Poskytnuté informace zajistí seznámení pracovníků objednatele se všemi podstatnými částmi dodávky v rozsahu potřebném pro obsluhu, provoz, údržbu a identifikaci nestandartních stavů systému a jejich příčin.
3) Vše uvedené bude probíhat v prostorách objednatele s využitím vybavení dodaného v rámci této veřejné zakázky, případně zajištěné ze strany objednatele.
4) Konkrétní termíny určí objednatel dle postupu v rámci realizace projektu a dostupnosti zainteresovaných osob.
5) Seznámení s funkcionalitami, obsluhou dodávaných technologií se týká klíčových uživatelů, ostatní uživatelé budou proškoleni klíčovými uživateli.

Veškeré náklady na zajištění těchto činností musí být zahrnuty v ceně odpovídající části předmětu dodávky.

4.6 ZÁRUKY

V této kapitole jsou uvedeny požadavky na záruky dodávky jako celku, případně specificky dílčích částí dodávky.

Objednatel požaduje záruku na veškeré dodané technologie včetně nezbytných provozních a servisních služeb v délce trvání minimálně:

a) 60 měsíců na informační systém(y), aplikace a služby spojené s realizací projektu,

b) 36 měsíců – u HW infrastruktury a systémového SW, pokud není u konkrétního vybavení uvedeno jinak. Delší záruka je uvedena jen u částí, kde je na trhu běžné poskytování delší záruky v pořizovací ceně.

c) 12 měsíců na spotřební materiál, případně drobné vybavení podléhající rychlému opotřebení. Případný spotřební materiál musí být explicitně označen v nabídce a smlouvě a musí být prokázáno, že splňuje tento charakter.

Záruka začíná běžet od okamžiku předání do ostrého (produkčního) provozu. Veškeré opravy po dobu záruky budou bez dalších nákladů pro provozovatele (objednatele). Veškeré komponenty, náhradní díly a práce budou poskytnuty bezplatně v rámci záruky. Zhotovitel ve své nabídce výslovně uvede všechny podmínky záruk.

a) Po dobu záruky na části dodávky musí zhotovitel nebo výrobce všech zařízení garantovat běžnou dostupnost náhradních komponentů a dostupnost servisu.

b) Součástí záruky je i shoda dodávaných systémů s platnou legislativou.

c) Max. doba na odstranění vady díla je 30 dnů od prokazatelného oznámení dodavateli.

d) Zhotovitel uvede provozní služby požadovaného předmětu plnění veřejné zakázky včetně parametrů, které budou předmětem dodávek v rámci záruky systému a v rámci poskytování servisních služeb.

Poskytovatel zajistí HelpDesk pro hlášení vad.

5 HARMONOGRAM

Následující tabulka obsahuje požadovaný časový harmonogram realizace dodávky (T ~ datum účinnosti smlouvy o dílo):

#	Fáze	Doba trvání od zahájení	Doplňující informace
1	Zahájení realizace	0	Zahájení realizace bude dnem podpisu smlouvy na dodávku.
2	Analýza a návrh řešení	45	Zpracování analýzy a návrhu řešení pro potřeby upřesnění podmínek realizace.
3	Dodávka, implementace, instalace, konfigurace HW a SW infrastruktury.	220	Dodávka a implementace HW, SW a síťové infrastruktury.
4	Vývoj a implementace úprav SW, dodávka dokumentace k SW.	220	Vlastní vývoj a implementace úprav IS dle analýzy a návrhu řešení.
5	Ověření funkčnosti dodaných technologií a systémů.	250	Otestování funkčnosti technologií a systémů a ověření jejich plné funkčnosti.
6	Seznámení s funkcionalitami, obsluhou dodávaných technologií	250	Seznámení s funkcionalitami, obsluhou dodávaných technologií
7	Dodávka dokumentace dodaného systému a jeho částí.	250	Min. uživatelská dokumentace, dokumentace skutečného provedení, systémová dokumentace, projektová dokumentace.
8	Převedení do zkušebního provozu.	251	Převedení do zkušebního provozu, odstranění všech vad a nedodělků, dokončení realizace a převedení do ostrého provozu.
9	Testování zranitelností / penetrační testy	280	Zpracování a předání testů zranitelností a penetračních testů a úpravy konfigurace bezpečnostních technologií tak, aby byly zjištěné zranitelnosti eliminovány. *Pozn.: jedná se o ověření správnosti nastavení bezpečnostních technologií v rámci dodávky,*
10	Ukončení realizace dodávky.	280	Součástí je zahájení doby provozu dodaného systému a poskytování servisních služeb.

Tabulka 47: Harmonogram

Doplňující informace:

- Pod pojmem „den“ je míněn kalendářní den.

- Zhotovitel má možnost definovat kratší termíny plnění (v rámci dodávky), v nabídce nelze zkrátit dobu zkušebního provozu, která musí být min. 10 dnů.
- Zkrácení zkušební doby je možné pouze na základě písemné dohody se Zadavatelem.

6 MÍSTA PLNĚNÍ

Realizace předmětu plnění bude probíhat v následujících místech plnění:

Místo	Adresa	Předmět realizace
Léčebna dlouhodobě nemocných Rybitví	Činžovních domů 140 Rybitví PSČ: 533 54	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Dodávky bezpečnostních technologií a související služby pro zabezpečení IS.
Vysokomýtská nemocnice	Hradecká 167 Vysoké Mýto PSČ: 566 23	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Dodávky bezpečnostních technologií a související služby pro zabezpečení IS.
	Žižkova 271 Vysoké Mýto PSČ: 566 23	Záložní datové centrum, umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Dodávky bezpečnostních technologií a související služby pro zabezpečení IS.
Nemocnice následné péře Moravská Třebová	Svitavská 25 Moravská Třebová PSČ: 571 16	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Dodávky bezpečnostních technologií a související služby pro zabezpečení IS.
Odborný léčebný ústav Jevíčko	Jevíčko 508 PSČ: 569 43	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Dodávky bezpečnostních technologií a související služby pro zabezpečení IS.
Albertinum, odborný léčebný ústav, Žamberk	Za Kopečkem 353 Žamberk PSČ: 564 21	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Dodávky bezpečnostních technologií a související služby pro zabezpečení IS.
Rehabilitační ústav Brandýs nad Orlicí	Lázeňská 58 Brandýs nad Orlicí, PSČ: 561 12	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Dodávky bezpečnostních technologií a související služby pro zabezpečení IS.
Nemocnice Pardubického kraje, a.s.	Kyjevská 44, Pardubice	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Dodávky bezpečnostních technologií a související služby pro zabezpečení IS.

Tabulka 48: Místa plnění

7 VÝCHOZÍ STAV

V této kapitole je uveden výchozí stav a výchozí podmínky pro dodávku předmětu plnění.

7.1 PARDUBICKÝ KRAJ (ZADAVATEL)

Pardubický kraj (PAK) na svém území zajišťuje poskytování zdravotní péče, a to od přednemocniční neodkladné péče, přes akutní péči až po následnou zdravotní péči pro občany a návštěvníky předmětného území s přesahem do okolních krajů.

Tato péče je zřizovanými (příspěvkové organizace) nebo zakládanými (a.s.) organizacemi, které poskytují tuto péči.

Pardubický kraj svými poskytovateli ZS poskytuje kvalitní komplexní zdravotní péči nejen pacientům na spádovém území Pardubického kraje, ale také dalším pacientům z jiných regionů, kteří o ně projevují zájem. Důraz je kladen na kvalitu poskytované zdravotní péče a bezpečí pacientů. Kvalita zdravotní péče se zvyšuje např. vybavením poskytovatelů ZS moderními technologiemi, a to jak zdravotnickými, tak i jinými (např. informačními).

Mimo poskytování kvalitní zdravotní péče je prioritou produktivita a efektivita činností, které je třeba podpořit moderními nástroji, a to i v oblasti informačních a komunikačních technologií, jak pro personál, tak pro pacienty.

Pardubický kraj musí zajistit výkon veřejné správy v uvedených oblastech a podmínky pro zajištění připravenosti poskytovatelů akutní lůžkové a následné zdravotní péče i v případě **kybernetických bezpečnostních událostí** (dle zákona č. Zákon č. 181/2014 Sb.).

Pro tyto činnosti poskytovatelé ZS a kraj využívají informační systémy a technologie (souhrnně „IS“):

1. Léčebna dlouhodobě nemocných Rybitví – Nemocniční informační systém – jedná se o primární IS sloužící pro hlavní činnost ZZ (správce), tj. pro poskytování následné zdravotní péče na území Pardubického kraje.
2. Odborný léčebný ústav Jevíčko – Nemocniční informační systém – jedná se o primární IS sloužící pro hlavní činnost ZZ (správce), tj. pro poskytování následné zdravotní péče na území Pardubického kraje.
3. Albertinum, odborný léčebný ústav Žamberk – Nemocniční informační systém – jedná se o primární IS sloužící pro hlavní činnost ZZ (správce), tj. pro poskytování následné zdravotní péče na území Pardubického kraje.
4. Nemocnice následné péče Moravská Třebová – Nemocniční informační systém – jedná se o primární IS sloužící pro hlavní činnost ZZ (správce), tj. pro poskytování následné zdravotní péče na území Pardubického kraje.
5. Vysokomýtská nemocnice – Nemocniční informační systém – jedná se o primární IS sloužící pro hlavní činnost ZZ (správce), tj. pro poskytování následné zdravotní péče na území Pardubického kraje.
6. Rehabilitační ústav Brandýs nad Orlicí – Nemocniční informační systém – jedná se o primární IS sloužící pro hlavní činnost ZZ (správce), tj. pro poskytování následné zdravotní péče na území Pardubického kraje.

V následujícím textu je uveden současný stav informačních systémů a technologií a další relevantní informace.

7.2 INFORMAČNÍ SYSTÉMY K ZABEZPEČENÍ

V rámci projektu budou realizována opatření k zabezpečení ostatních [2] informačních systémů (IS) poskytovatelů ZS Pardubického kraje. V rámci projektu nebudou realizována opatření k zabezpečení kritické informační infrastruktury (KII), žádného informačního systému základních služeb (ISZS) ani žádného významného informačního systému.

Pardubický kraj bude zabezpečovat informační systémy (IS) svých poskytovatelů ZS. Stručný výčet IS je uveden v dalším textu této kapitoly.

Všechny uvedené IS jsou umístěny, provozovány a využívány uživateli v sídlech poskytovatelů ZS Pardubického kraje nebo na adresách na území Pardubického kraje uvedených v kap. 6.

Bezpečnostní technologie budou umístěny do uvedených datových center, rozvodných místností a na pracoviště uživatelů těchto IS tak, aby byla zajištěna provozuschopnost a bezpečnost provozovaných IS i v případě kybernetických bezpečnostních událostí, mimořádných událostí a krizových situací.

Předmětem projektu bude zabezpečení ostatních [3] informačních systémů (IS) dle SPPŽP, tj. jedná se o systémy, které nespadají pod KII/VIS/ISZS, a které spravuje žadatel.

Správcem dále uvedených IS je vždy konkrétní poskytovatel ZS Pardubického kraje. Pardubický kraj je vlastníkem jak poskytovatelů ZS, tak IS jim svěřených a jimi spravovaných, tj. je oprávněným žadatelem, protože zabezpečuje své IS. Pardubický kraj tedy plní podmínky oprávněného žadatele.

Žádný ze zabezpečovaných IS, ani žádná z jejich součástí, netvoří systém určený k ochraně utajovaných skutečností dle zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti (ISOUI).

Uvedené IS nejsou informačními systémy základní služby podle §2, písm. i), bod 5 a písm. j) ZKB a vyjmenovaní poskytovatele ZS Pardubického kraje nebyli Národním úřadem pro kybernetickou a informační bezpečnost určeni jako provozovatelé základní služby podle §22a ZKB.

V následující tabulce je uveden výčet IS, které jsou určeny k zabezpečení a vůči nimž budou realizována technická opatření:

Název IS	Správce	Stručný popis	Typ
Nemocniční informační systém	Léčebna dlouhodobě nemocných Rybitví	Informační systém a technologie pro podporu činností zdravotnického zařízení, tj. poskytování zdravotní péče. Jedná se o soubor technologií a subsystémů společně zajišťující podporu uvedených procesů. Jedná se o primární IS sloužící pro hlavní činnost ZZ (správce), tj. pro poskytování zdravotní péče.	Informační systém (IS)
Nemocniční informační systém	Odborný léčebný ústav Jevíčko	Informační systém a technologie pro podporu činností zdravotnického zařízení, tj. poskytování zdravotní péče. Jedná se o soubor technologií a subsystémů společně zajišťující podporu uvedených procesů.	Informační systém (IS)

[2] „Ostatní" odpovídá terminologii Výzvy.
[3] „Ostatní" odpovídá terminologii Výzvy.

Název IS	Správce	Stručný popis	Typ
		Jedná se o primární IS sloužící pro hlavní činnost ZZ (správce), tj. pro poskytování zdravotní péče.	
Nemocniční informační systém	Albertinum, odborný léčebný ústav Žamberk	Informační systém a technologie pro podporu činností zdravotnického zařízení, tj. poskytování zdravotní péče. Jedná se o soubor technologií a subsystémů společně zajišťující podporu uvedených procesů. Jedná se o primární IS sloužící pro hlavní činnost ZZ (správce), tj. pro poskytování zdravotní péče.	Informační systém (IS)
Nemocniční informační systém	Nemocnice následné péče Moravská Třebová	Informační systém a technologie pro podporu činností zdravotnického zařízení, tj. poskytování zdravotní péče. Jedná se o soubor technologií a subsystémů společně zajišťující podporu uvedených procesů. Jedná se o primární IS sloužící pro hlavní činnost ZZ (správce), tj. pro poskytování zdravotní péče.	Informační systém (IS)
Nemocniční informační systém	Vysokomýtská nemocnice	Informační systém a technologie pro podporu činností zdravotnického zařízení, tj. poskytování zdravotní péče. Jedná se o soubor technologií a subsystémů společně zajišťující podporu uvedených procesů. Jedná se o primární IS sloužící pro hlavní činnost ZZ (správce), tj. pro poskytování zdravotní péče.	Informační systém (IS)
Nemocniční informační systém	Rehabilitační ústav Brandýs nad Orlicí	Informační systém a technologie pro podporu činností zdravotnického zařízení, tj. poskytování zdravotní péče. Jedná se o soubor technologií a subsystémů společně zajišťující podporu uvedených procesů. Jedná se o primární IS sloužící pro hlavní činnost ZZ (správce), tj. pro poskytování zdravotní péče.	Informační systém (IS)

Tabulka 49: Výčet IS k zabezpečení

7.2.1 Provoz

7.2.1.1 Provoz řešení

Provoz řešení bude zajišťovat Pardubický kraj a jeho ZZ v rámci svých běžných provozních činnosti v uvedených datových centrech (primární i záložní) a v rámci uvedených datových center (primární i záložní).

Všechna datová centra jsou provozována v režimu 365x7x24, tj. nonstop.

V rámci provozu bude zajištěno:

1. Administrace řešení – např. oprávnění, správa zdrojů apod.

2. Dohled nad řešením, případně jeho částmi.
3. Zálohování řešení (data, konfigurace, SW infrastruktura).
4. 1st level support, vyhodnocení hlášených problémů a předávání závad na technickou a technologickou podporu dodavatele.
5. Bude využívána Regionální datová síť (RDS), přes kterou budou předávána data z bezpečnostních technologií do SOC, SIEM a dalších nadřazených bezpečnostních technologií a systémů.

V rámci provozu mohou být řešeny i další služby, které budou zajištěny buď pracovníky žadatele, nebo smluvně u poskytovatele služeb nad rámci této VZ.

7.2.1.1.1 Technická a technologická podpora

Technická a technologická podpora projektu bude zajištěna v následujícím rozsahu:

1. V režimu 7x24x365 – nemocniční systémy poskytovatelů ZS jsou kritickými systémy, jejichž služby jsou uživatelům k dispozici nonstop, protože poskytovatelé ZS poskytují služby a plní své úkoly nonstop.
2. Součástí dodávky technických opatření (technologií) bude maintenance technologií a dodaných technologií, technická a technologická podpora nad rámec záruky s kratšími SLA než v případě záruky.
3. Součástí technické podpory budou:
    a. Nezbytné úpravy nastavení technologií vyplývající ze změn legislativy, vyhlášek, případně dalších závazných dokumentů.
    a. Pozáruční servis HW a SW infrastruktury.

Zajištění provozu u stávajících IS a technologií musí být zachováno min. v tomto rozsahu.

KONEC DOKUMENTU

Příloha č. 3: Servisní služby

V této příloze jsou uvedeny výchozí podmínky a požadavky na servisní služby v rámci této veřejné zakázky.

OBSAH

SEZNAM PŘÍLOH

Nejsou.

VYUŽITÉ ZDROJE

[1] Technická specifikace

SEZNAM TABULEK

SEZNAM ZKRATEK A POJMŮ

Zkratka/pojem	Význam
24 x 7	Poskytování služeb 365 dní v roce, 24 hodiny denně, 7 dnů v týdnu
5 x 10	Poskytování služeb v pracovní dny, v pracovní době, 10 hodin denně
DB	Databáze
DC	Datové centrum
EU	Evropská unie
HW	Hardware
ICT	Informační a komunikační technologie
IS	Informační systém
OS	Operační systém
PAK	Pardubický kraj
PD	Projektová dokumentace
SLA	Úroveň a podmínky poskytování služeb technické a technologické podpory.
SoD	Smlouva o dílo
SW	Software
VŘ	Výběrové řízení
VZ	Veřejná zakázka
ZD	Zadávací dokumentace nebo zdravotnická dokumentace (dle kontextu)
ZVZ	Zákon o zadávání veřejných zakázek

Tabulka 1: Seznam zkratek a pojmů

1 PŘEDMĚT PLNĚNÍ

Předmětem plnění veřejné zakázky (dílem) je komplexní dodávka a implementace technologií, dodávky SW, HW a infrastruktury pro realizaci technických bezpečnostních opatření dle § 5 odst. 3) zákona č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB) pro zabezpečení NIS provozovaných poskytovateli zdravotních služeb následné péče zřizovaných Pardubickým krajem (žadatel) v rámci výkonu veřejné správy v oblasti poskytování zdravotní péče, kterou Pardubický kraj vykonává na území Pardubického Součástí plnění VZ jsou dále servisní služby po dobu udržitelnosti projektu.

Součástí plnění VZ jsou dále provozní a servisní služby pro zajištění provozu dodaných systémů, jejich úprav a technologií na dobu 5 let.

Předmětem plnění této smlouvy je poskytování servisních služeb dodaných bezpečnostních technologií, úprav informačních systémů, provozních technologií, SW, systémového SW, HW a komunikační infrastruktury a související vybavení dodaných v rámci díla realizovaného v rámci smlouvy o dílo (dále jen „SoD“) na dobu 5 let od dodání díla.

Pro potřeby tohoto dokumentu je dále využíván souhrnný název „Systém“ pro všechny součástí dodávky dle SoD.

Předmět plnění je tedy následující:

1. Zajištění technické a technologické podpory a nezbytných servisních služeb dodaných bezpečnostních technologií.
2. Uvedené služby jsou nad rámec záruky, jak je definována ve SoD.
3. Služby budou poskytovány v režimu uvedeném v následujícím textu dle požadované dostupnosti příslušné části řešení.
4. Součástí bude maintenance technologií a dodaného SW, technická a technologická podpora nad rámec záruky s kratšími SLA než v případě záruky – SLA jsou specifikována dále v tomto dokumentu.
5. Nezbytné úpravy systému vyplývající ze změn legislativy, vyhlášek, případně dalších závazných dokumentů.
6. Pozáruční servis provozní infrastruktury a SW infrastruktury.
7. Rozšířená podpora pro řešení dodatečných požadavků na provoz bezpečnostních technologií.

2 VÝCHOZÍ STAV

Výchozí stav díla pro poskytování servisních služeb je dán dodaným dílem v rámci Smlouvy o dílo.

Zahájení plnění dle této smlouvy je ode dne předání a akceptace díla dle smlouvy o dílo.

3 POŽADAVKY NA SLUŽBY

V této kapitole jsou uvedeny požadavky na servisní služby, tj. maintenance a základní podpora a rozšířená podpora technologií a IS dodaných v rámci smlouvy o dílo.

3.1 KATEGORIE SLUŽEB

V rámci zabezpečení provozu jsou požadovány následující služby k Systému:

1. Provoz a zajištění dostupnosti
2. Maintenance a základní podpora
3. Rozšířená podpora

Požadavky a parametry služeb jsou uvedeny v následujícím textu.

3.2 MAINTENANCE A ZÁKLADNÍ PODPORA

V této kapitole je uvedena specifikace služeb maintenance a základní podpory.

3.2.1 Poskytované služby

Jsou požadovány následující služby:

1. Poskytování služby HelpDesk včetně základní servisní technické podpory Systému při odstraňování závad Systému. HelpDesk bude k dispozici pracovní dny v režimu 5 x 10, nicméně služby budou poskytovány dle úrovně v kap. 4 – Úroveň požadovaných služeb.
2. Poskytování pravidelné profylaxe Systému vč. indikace a předcházení možných problémů při užívání Systému min. 1x ročně.
3. Zajištění souladu funkčnosti a vlastností systému s aktuální legislativou vč. bezplatného provádění nezbytných úprav systémů pro splnění tohoto požadavku.
4. Dokumentace k aktualizacím Softwarových produktů a technologií, aktualizace provozní dokumentace Systému tak, aby odpovídala aktuálnímu stavu provozovaného Systému.
5. Aplikace service packů a hotfixů nutných pro bezchybný chod systému, které byly identifikovány na základě profylaxe a jejich aplikace byla dohodnuta za úplatu na základě objednávky Objednatele.

Výčet Softwarových produktů a technologií, na které se vztahují servisní služby je v kap. 4 – Úroveň požadovaných služeb.

3.2.2 Podmínky poskytování služeb

Druhy poruch:

P1. Porucha kategorie P1 – Urgentní – za Urgentní poruchu se považuje stav:

   a. celkové nefunkčnosti systému a nemožnost využívat klíčové funkcionality řešení nadpolovičním počtem všech uživatelů.

   b. Závažné porušení bezpečnosti – přístup k systému a datům bez autentifikace, či autorizace (obejití přístupových práv); neoprávněný přístup k technickým prostředkům; neoprávněné zacházení s daty (přístup neodpovídající přiřazené roli v systému); přihlášení do sytému pomocí neplatných certifikátů, či hesel; přístup k systému (jiným systémem, nebo fyzickou osobou) pomocí jiných služeb než definovaných; a jiné, které ohrožují integritu, důvěryhodnost, či neodvolatelnost uložených a poskytovaných dat.

P2. Porucha kategorie P2 – Běžná – za Běžnou poruchu se považuje stav, který neodpovídá požadavkům ZD, schválené implementační analýze nebo platné dokumentaci, případně bezpečnostní problémy mimo úroveň P1, ale neohrožují klíčové funkcionality řešení, systém je možné provozovat v omezeném rozsahu, neohrožujícím jeho věrohodnost a zajišťujícím kompletnost a úplnost zpracovávaných dat

Řešení poruch:

1. V případě, že se jedná o poruchu na Systému dle této Smlouvy, vztahují se na ni SLA dle této Smlouvy.
2. V případě, že se jedná o poruchu integrovaného systému nebo HW a SW infrastruktury mimo tuto Smlouvu s dopadem na Systém uvedený v této Smlouvě, nevztahují se na tuto poruchu SLA dle této Smlouvy do doby odstranění poruchy integrovaného systému nebo infrastruktury.
3. V případě, že bude snížena závažnost poruchy, snižují se poměrně k tomuto SLA a lhůty ve vztahu k nové závažnosti poruchy.
4. Poskytovatel je oprávněn navrhnout nebo poskytnout náhradní řešení poruchy tak, aby došlo k eliminaci dopadů této poruchy na provoz ZZS (snížení závažnosti nebo omezení poruchy) do konečného systémového řešení.
5. Dohodnou-li se obě strany na provedení zásahu v termínu po lhůtě na odstranění poruchy, nebude toto považováno za nedodržení lhůty na odstranění poruchy ze strany Poskytovatele. Taková dohoda musí být dokumentována v rámci popisu řešení dané poruchy a oprávněnost jejího použití vzniká po jejím schválení odpovědným zástupcem Objednatele (žadatel, případně vedoucí projektu).

Způsob ohlašování poruch:

Poruchy Objednatel (oprávněné osoby Objednatele) hlásí na kontaktní místo Poskytovatele (Help Desk) prostřednictvím elektronického systému pro správu požadavků (helpdesk).

Poruchy kategorie P1 objednatel vždy hlásí telefonicky a doplňující informace poskytuje prostřednictvím helpdesku nebo elektronickou poštou. Kontaktní údaje a oprávněné osoby Objednatele jsou uvedeny v samostatné příloze smlouvy.

Poruchy nahlášené telefonicky nebo emailem budou zaznamenány do helpdesku.

Poruchy budou do systému zadávány jednotlivě – samostatné hlášení pro každou závadu.

Reakce Poskytovatele:

Služba Help Desk Poskytovatele dle sjednané reakční doby potvrdí Objednateli , že obdržela výzvu Objednatele k odstranění poruchy. V potvrzení uvede označení evidované poruchy a zahájení prací na odstraňování poruchy. Tyto informace doručí osobě, která problém za Objednatele nahlásila (dále jen Žadatel) a pracovišti Helpdesku Objednatele.

Lhůta na odstranění poruchy

Konečná lhůta na odstranění poruchy je dána okamžikem ohlášení poruchy Objednatelem (oprávněnou osobou Objednatele) do doby vyřešení poruchy.

Režimy

- 5 x 10 – poskytování služeb v pracovní dny, v pracovní době

Pracovní dny: pondělí – pátek, vyjma státních svátků, pracovní doba v pracovních dnech od 7:00 do 16:00 h.

Lhůty

Porucha	Režim	Zahájení odstraňování poruchy (reakční doba)	Lhůta na odstranění poruchy
P1	5 x 10	4 hodiny v pracovní době	2 pracovní dny
P2	5 x 10	3 pracovní dny	20 pracovních dnů

V případě poruchy, která pominula, a není možné identifikovat při prvotním výskytu její příčinu (neexistují logy, nejsou podklady od Objednatele) a potřeby monitoringu v delším časovém úseku, bude zadaná porucha na helpdesku po vzájemné dohodě mezi Poskytovatelem a Objednatelem převedena do specifické kategorie pro tento účel – kategorie „Odloženo“. V případě opakovaného výskytu bude porucha znovu otevřena (k datu nahlášení) a řešena v souladu s dohodnutými SLA. Poskytovatel je povinen vyvinout aktivitu k identifikaci příčiny chyby již po prvním výskytu. Při jejím opakovaném výskytu platí v plném rozsahu dohodnutá SLA, lhůta k odstranění počíná běžet okamžikem ohlášení druhého výskytu.

V případě poruch provozní infrastruktury, systémového software či informačního systému Objednatele se Poskytovatel zavazuje zajistit za úhradu na základě objednávky Objednatele reinstalaci Systému a zálohovaných dat na novou provozní infrastrukturuObjednatele.

3.2.3 Ostatní podmínky

Ostatní podmínky na poskytování maintenance a základní podpory jsou:

1. Případné Servisní výjezdy (práce a cestovní náklady) na území Pardubického budou Poskytovatelem Objednateli účtovány.
2. Legislativní úpravy systému v návaznosti na změny legislativy, vyhlášek a nařízení ČR a EU a zdravotních pojišťoven – v rámci paušální platby.
3. Poskytování součinnosti dalším poskytovatelům služeb zabezpečení provozu integrovaných systémů v rámci poskytování maintenance nebo základní podpory v rámci zabezpečení provozu.
4. V rámci provozu Systému bude v součinnosti Objednatele a Poskytovatele docházet na základě požadavku Objednatele k instalacím nových verzí SW, bezpečnostních a opravných balíčků systémového SW (OS, DB apod.) . Služby budou na Systém poskytovány, pokud bude zajištěno ve vzájemné součinnosti s Poskytovatelem nebo nebudou v rozporu se standardními požadavky na chod Systému.

3.3 ROZŠÍŘENÁ PODPORA

Jedná se o služby na základě požadavku Objednatele pro řešení dodatečných požadavků na provoz a využívání Systému nad rámec záruky a ostatních uvedených služeb.

3.3.1 Požadované služby

Jsou požadovány následující služby:

1. Analytické a konzultační služby k Systému.
2. Reporting a analýza dat Systému.
3. Součinnost při řešení systémových problémů a při implementaci systémů třetích stran.
4. Další Zadavatelem požadované Služby ve vazbě na Systém – datové práce v systému, kontrola běhu systému, zakládání uživatelů, ostatní servisní činnosti nad rámec základní technické podpory.

5. Aktualizace stávající dokumentace Systému o nově dodané či změněné funkce Systému.

3.3.2 Rozsah poskytovaných služeb

Rozsah poskytovaných služeb je následující:

1. 24 hodin / 1 kalendářní čtvrtletí.
2. Nevyčerpané hodiny v rámci jednotlivých čtvrtletí jsou kumulativně převoditelné maximálně do 1 roku od vzniku jejich nároku, následně nárok na nevyčerpané služby zaniká.

3.3.3 Podmínky poskytování služeb

Služby budou poskytovány následujícím způsobem:

1. Objednatel (kontaktní osoba) předloží výzvu na Poskytovatele (kontaktní osobu) obsahující specifikaci požadovaných služeb rozšířené podpory, včetně požadovaného termínu plnění.
2. Poskytovatel předloží Objednateli nabídku na poskytnutí požadovaných služeb.
    a. Předložení nabídky Objednateli do 30 kalendářních dnů. Lhůta je závazná a její nesplnění bude pokutováno v souladu se Smlouvou.
    b. Nabídka bude oceněna počtem hodin a sazbou dle položkového rozpočtu, který je samostatnou přílohou Smlouvy.
    c. Pokud požadované služby budou vyžadovat jakékoliv související náklady nad rámec služeb rozšířené podpory (rozšíření licencovaného SW apod.) bude toto nabídka obsahovat včetně nacenění a zdůvodnění.
    d. Platnost nabídky bude min. 30 kalendářních dnů.
3. Pokud se Objednatel rozhodne, že přijme nabídku Poskytovatele, zašle Poskytovateli výzvu k poskytnutí služeb dle nabídky („Dílčí objednávku“).
4. Poskytovatel do 5 pracovních dnů potvrdí přijetí Dílčí objednávky k poskytnutí služeb a zahájí poskytování v souladu se svou nabídkou a Dílčí objednávkou. Poskytovatel není oprávněn nepřijmout Dílčí objednávku, pokud nedošlo ke změně rozsahu poskytovaných služeb nebo neuplynula doba platnosti nabídky Poskytovatele.
5. Přijetím Dílčí objednávky se termíny dle nabídky Poskytovatele stávají závaznými a jejich nesplnění bude pokutováno v souladu se Smlouvou.
6. Tyto služby budou odsouhlaseny v rámci akceptace plnění Dílčí objednávky.

4 ÚROVEŇ POŽADOVANÝCH SLUŽEB

V následující tabulce je uvedena úroveň požadovaných služeb k jednotlivým částem dodávky:

#	Položka rozpočtu	Režim poskytování	Doplňující informace	ID[1]
1	**Pardubický kraj**			
1.1	Rozšíření systému pro sběr a analýzu logů v NPK	5 x 10		1.1 1.2
1.2	Zpracování událostí z analýzy síťového provozu ZZ v NPK	5 x 10		1.1 1.2
1.3	Zpracování událostí ze skenování perimetru ZZ v NPK	5 x 10		1.1 1.2
2	**Léčebna dlouhodobě nemocných Rybitví (LDN Rybitví)**			
2.1	Nástroje monitorování a bezpečnost počítačových sítí	5 x 10		2.2
2.2	Nástroje pro ochranu síťového perimetru	5 x 10		2.3
2.3	Redundantní infrastruktura pro záložní DC pro provoz zabezpečovaného IS – HW	5 x 10		2.4
2.4	Systémový SW pro redundantní infrastrukturu pro záložní DC pro provoz zabezpečovaného IS – SW	5 x 10		2.5
2.5	Dodávka Anti-X řešení pro ochranu před škodlivým kódem	5 x 10		2.6
2.6	Nástroje pro sběr logů a významných provozních událostí	5 x 10		2.7
2.7	Infrastruktura pro provoz bezpečnostních technologií	5 x 10		2.8
2.8	Systémový SW pro provoz bezpečnostních technologií	5 x 10		2.9
3	**Odborný léčebný ústav Jevíčko (OLU Jevíčko)**			
3.1	Nástroje pro ochranu síťového perimetru a vnitřní sítě	5 x 10		3.2
3.2	Nástroje monitorování a bezpečnost počítačových sítí	5 x 10		3.3

[1] Jedná se o pomocné interní označení příslušnosti do položky v rozpočtu projektu bez specifického významu pro VZ.

#	Položka rozpočtu	Režim poskytování	Doplňující informace	ID[1]
3.3	Dvoufaktorová autentizace administrátorských VPN přístupů	5 x 10		3.4
3.4	Zálohovací infrastruktura pro záložní DC pro zálohování dat a technologií zabezpečovaného IS – HW	5 x 10		3.5
3.5	Nástroje pro sběr logů a významných provozních událostí	5 x 10		3.6
3.6	Infrastruktura pro provoz bezpečnostních technologií	5 x 10		3.7
3.7	Systémový SW pro provoz bezpečnostních technologií	5 x 10		3.8
4	**Albertinum, odborný léčebný ústav Žamberk (OLÚ Albertinum Žamberk)**			
4.1	Nástroje pro ochranu síťového perimetru	5 x 10		4.3
4.2	Redundantní infrastruktura pro záložní DC pro provoz zabezpečovaného IS – HW	5 x 10		4.4
4.3	Systémový SW pro redundantní infrastrukturu pro záložní DC pro provoz zabezpečovaného IS – SW	5 x 10		4.5
4.4	Dodávka Anti-X řešení pro ochranu před škodlivým kódem	5 x 10		4.6
4.5	Nástroje pro sběr logů a významných provozních událostí	5 x 10		4.7
4.6	Infrastruktura pro provoz bezpečnostních technologií	5 x 10		4.8
4.7	Systémový SW pro provoz bezpečnostních technologií	5 x 10		4.9
5	**Nemocnice následné péče Moravská Třebová (NNP Moravská Třebová)**			
5.1	Nástroje pro ochranu síťového perimetru	5 x 10		5.2
5.2	Nástroje pro identifikaci, autentizaci a řízení oprávnění uživatelů a administrátorů – SW	5 x 10		5.4
5.3	Nástroje monitorování a bezpečnost počítačových sítí	5 x 10		5.5
5.4	Nástroje pro sběr logů a významných provozních událostí	5 x 10		5.6

#	Položka rozpočtu	Režim poskytování	Doplňující informace	ID[1]
5.5	Redundantní infrastruktura pro záložní DC pro provoz zabezpečovaného IS a bezpečnostních technologií – HW	5 x 10		5.7
5.6	Systémový SW pro redundantní infrastrukturu pro záložní DC pro provoz zabezpečovaného IS a bezpečnostních technologií – SW	5 x 10		5.8
6	**Vysokomýtská nemocnice (NVM)**			
6.1	Rozšíření Anti-X řešení pro ochranu před škodlivým kódem	5 x 10		6.2
6.2	Nástroje pro ochranu síťového perimetru	5 x 10		6.4
6.3	Nástroje pro segmentaci sítí a řízení přístupu k síti	5 x 10		6.5
6.4	Nástroje monitorování a bezpečnost počítačových sítí	5 x 10		6.6
6.5	Řízení přístupu uživatelů a administrátorů	5 x 10		6.7
6.6	Zálohovací infrastruktura pro záložní DC pro zálohování dat a technologií zabezpečovaného IS – HW	5 x 10		6.8
6.7	Software pro zálohovací infrastrukturu pro záložní DC pro zálohování dat a technologií zabezpečovaného IS – SW	5 x 10		6.9
6.8	Nástroje pro sběr logů a významných provozních událostí	5 x 10		6.10
6.9	Infrastruktura pro provoz bezpečnostních technologií	5 x 10		6.11
6.10	Systémový SW pro provoz bezpečnostních technologií	5 x 10		6.12
7	**Rehabilitační ústav Brandýs nad Orlicí (RÚ BnO)**			
7.1	Nástroje pro ochranu síťového perimetru	5 x 10		7.2
7.2	Nástroje monitorování a bezpečnost počítačových sítí	5 x 10		7.3
7.3	Redundantní infrastruktura pro záložní DC pro provoz zabezpečovaného IS – HW	5 x 10		7.4

#	Položka rozpočtu	Režim poskytování	Doplňující informace	ID[1]
7.4	Systémový SW pro redundantní infrastrukturu pro záložní DC pro provoz zabezpečovaného IS – SW	5 x 10		7.5
7.5	Nástroje pro sběr logů a významných provozních událostí	5 x 10		7.6
7.6	Infrastruktura pro provoz bezpečnostních technologií	5 x 10		7.7
7.7	Systémový SW pro provoz bezpečnostních technologií	5 x 10		7.8
8	**Ostatní systémy a technologie**			
8.1	Nástroje pro penetrační testy a penetrační testy	Jen záruka		V.2

Tabulka 2: Úroveň požadovaných služeb

5 MÍSTA PLNĚNÍ

Realizace předmětu plnění bude probíhat v následujících místech plnění:

Místo	Adresa	Předmět realizace
Léčebna dlouhodobě nemocných Rybitví	Činžovních domů 140 Rybitví PSČ: 533 54	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Poskytování servisních služeb pro bezpečnostní technologie a zabezpečené IS.
Vysokomýtská nemocnice	Hradecká 167 Vysoké Mýto PSČ: 566 23	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Poskytování servisních služeb pro bezpečnostní technologie a zabezpečené IS.
	Žižkova 271 Vysoké Mýto PSČ: 566 23	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Poskytování servisních služeb pro bezpečnostní technologie a zabezpečené IS.
Nemocnice následné péře Moravská Třebová	Svitavská 25 Moravská Třebová PSČ: 571 16	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Poskytování servisních služeb pro bezpečnostní technologie a zabezpečené IS.
Odborný léčebný ústav Jevíčko	Jevíčko 508 PSČ: 569 43	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Poskytování servisních služeb pro bezpečnostní technologie a zabezpečené IS.
Albertinum, odborný léčebný ústav, Žamberk	Za Kopečkem 353 Žamberk PSČ: 564 21	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Poskytování servisních služeb pro bezpečnostní technologie a zabezpečené IS.
Rehabilitační ústav Brandýs nad Orlicí	Lázeňská 58 Brandýs nad Orlicí, PSČ: 561 12	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Poskytování servisních služeb pro bezpečnostní technologie a zabezpečené IS.
Nemocnice Pardubického kraje, a.s.	Kyjevská 44, Pardubice	Umístění zabezpečovaného IS, včetně provozní infrastruktury a souvisejících technologií. Poskytování servisních služeb pro bezpečnostní technologie a zabezpečené IS.

Tabulka 3: Místa plnění

6 OSTATNÍ PODMÍNKY

Kvalita a záruky:

1. Kvalita služeb bude zcela odpovídat požadavkům kladeným na HW i SW ve shodě s touto Zadávací dokumentací.
2. Poskytovatel se bude zavazovat provádět služby v kvalitě odpovídající účelu této Smlouvy, obecně závazným předpisům a platným technickým normám.
3. Poskytovatel nebude odpovídat za jakékoli škody vzniklé Objednateli, ani za neplnění nebo zpožděné plnění svých povinností vyplývajících ze Smlouvy, dojde-li k nim v důsledku působení vyšší moci. Působením vyšší moci se rozumí okolnosti vylučující odpovědnost podle Zákona č. 89/2012 Sb., občanského zákoníku, zejména pak negativní vliv takové škody v době platnosti Smlouvy, nepředvídatelné události (živelná pohroma, průmyslová katastrofa, ozbrojený konflikt, revoluce nebo obdobná změna státního režimu), jejichž výskyt a vliv podstatně působí na plnění Smlouvy, aniž by tomuto vlivu Objednatel a/nebo Poskytovatel mohli s použitím veškerých jim právně dostupných a rozumně požadovatelných prostředků účinně zabránit.

Obnova dat, bezpečnost a pravidla pro update aplikace:

1. Poskytovatel nebude odpovědný za ztrátu nebo změnu dat při provozu počítačového systému Objednatele způsobenou používáním systému v rozporu s projektovou dokumentací. Případnou obnovu dat bude provádět Poskytovatel ze záloh dat Objednatele.
2. Nové verze technologií budou Poskytovatelem předány Objednateli k ověření deklarované funkčnosti. Vlastní implementace nebo instalace bude provedena Poskytovatelem po odsouhlasení Objednatelem. Toto se netýká odstranění závad v rámci plnění základní podpory.

Servis vybavení prováděný pracovníky Objednatele:

1. Pracovníkům Objednatele bude umožněno provádět drobné opravy závad vybavení vlastními silami při dodržení všech závazných podmínek a ustanovení jakož i veškerých pracovních postupů a doporučení stanovených Poskytovatelem.
2. Pracovník Objednatele bude povinen vyžádat si souhlas Poskytovatele v každém případě, kdy nebude zcela jisté, zda bude oprávněn provést danou opravu vlastními silami a současně si vyžádat doporučení vhodného postupu provedení opravy. Souhlas Poskytovatele i jím doporučený pracovní postup musí být zaevidován v helpdesku, provozovaném Poskytovatelem.
3. Stejně tak veškeré informace o zjištěných závadách a provedených opravách bude Objednatel povinen řádně evidovat prostřednictvím helpdesku, provozovaného Poskytovatelem.
4. Za opravy provedené pracovníky Objednatele neponese Poskytovatel žádnou zodpovědnost a na tyto opravy nebude poskytovat žádné záruky. Poskytovatel dále neponese žádnou zodpovědnost za jakékoli závady nebo škody, způsobené pracovníky Objednatele při provádění oprav vybavení. Tyto závady nebude možné považovat za chyby informačního systému a případné odstranění těchto závad Poskytovatelem bude placenou službou.

7 SPECIFICKÉ ÚDAJE POSKYTOVATELE

Údaj	Hodnota
Helpdesk *(odkaz na elektronický systém pro správu požadavků):*	*<doplní poskytovatel v rámci své nabídky, tento text poté smaže>*
E-mail *(alternativní způsob hlášení poruch):*	*<doplní poskytovatel v rámci své nabídky, tento text poté smaže>*
Telefon *(alternativní způsob hlášení poruch):*	*<doplní poskytovatel v rámci své nabídky, tento text poté smaže>*
Jednotková cena pro rozšířenou podporu *(v Kč bez DPH)*:	*<doplní poskytovatel v rámci své nabídky, tento text poté smaže>*

Tabulka 4: Specifické údaje Poskytovatele

Podmínky provozu Systému v rámci provozní infrastruktury:

<Doplní poskytovatel v rámci své nabídky.

Z popisu musí být zřejmé, že pro Objednatele nevznikají v rámci dodávky ani provozu žádné náklady nad rámec plateb v rámci této servisní služby.

Tento text poté smaže>

KONEC ZÁKLADNÍ ČÁSTI DOKUMENTU

Příloha č. 4: Položkový rozpočet - nabídková cena

Položka ceny	Cena v Kč bez DPH	DPH v Kč	Cena v Kč s DPH
Celková nabídková cena za dodávky dle vzorové Smlouvy o dílo	0,00 Kč	0,00 Kč	0,00 Kč
Celková nabídková cena za servisní služby dle vzorové Servisní smlouvy	0,00 Kč	0,00 Kč	0,00 Kč
Celková nabídková cena za plnění této VZ (dodávky i servisní služby)	**0,00 Kč**	**0,00 Kč**	**0,00 Kč**

Ozn.	Položka rozpočtu	Jednotka	Počet jednotek	Jednotková cena (v Kč bez DPH)	Cena za dodávku (v Kč bez DPH)	Cena za dodávku (v Kč s DPH)	Cena za servisní služby / 1 kalendářní čtvrtletí (v Kč bez DPH)	Cena za servisní služby / 5 let (v Kč bez DPH)	Cena za servisní služby / 5 let (v Kč s DPH)
1	**Pardubický kraj**								
1.1	Rozšíření systému pro sběr a analýzu logů v NPK	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
1.2	Zpracování událostí z analýzy síťového provozu ZZ v NPK	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
1.3	Zpracování událostí ze skenování perimetru ZZ v NPK	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
2	**Léčebna dlouhodobě nemocných Rybitví (LDN Rybitví)**								
2.1	Nástroje monitorování a bezpečnost počítačových sítí	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
2.2	Nástroje pro ochranu síťového perimetru	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
2.3	Redundantní infrastruktura pro záložní DC pro provoz zabezpečovaného IS – HW	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
2.4	Systémový SW pro redundantní infrastrukturu pro záložní DC pro provoz zabezpečovaného IS – SW	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
2.5	Dodávka Anti-X řešení pro ochranu před škodlivým kódem	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
2.6	Nástroje pro sběr logů a významných provozních událostí	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
2.7	Infrastruktura pro provoz bezpečnostních technologií	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
2.8	Systémový SW pro provoz bezpečnostních technologií	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
3	**Odborný léčebný ústav Jevíčko (OLU Jevíčko)**								
3.1	Nástroje pro ochranu síťového perimetru a vnitřní sítě	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
3.2	Nástroje monitorování a bezpečnost počítačových sítí	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
3.3	Dvoufaktorová autentizace administrátorských VPN přístupů	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
3.4	Zálohovací infrastruktura pro záložní DC pro zálohování dat a technologií zabezpečovaného IS – HW	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
3.5	Nástroje pro sběr logů a významných provozních událostí	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
3.6	Infrastruktura pro provoz bezpečnostních technologií	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
3.7	Systémový SW pro provoz bezpečnostních technologií	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
4	**Albertinum, odborný léčebný ústav Žamberk (OLÚ Albertinum Žamberk)**								
4.1	Nástroje pro ochranu síťového perimetru	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
4.2	Redundantní infrastruktura pro záložní DC pro provoz zabezpečovaného IS – HW	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
4.3	Systémový SW pro redundantní infrastrukturu pro záložní DC pro provoz zabezpečovaného IS – SW	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
4.4	Dodávka Anti-X řešení pro ochranu před škodlivým kódem	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
4.5	Nástroje pro sběr logů a významných provozních událostí	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
4.6	Infrastruktura pro provoz bezpečnostních technologií	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
4.7	Systémový SW pro provoz bezpečnostních technologií	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
5	**Nemocnice následné péče Moravská Třebová (NNP Moravská Třebová)**								
5.1	Nástroje pro ochranu síťového perimetru	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
5.2	Nástroje pro identifikaci, autentizaci a řízení oprávnění uživatelů a administrátorů – SW	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
5.3	Nástroje monitorování a bezpečnost počítačových sítí	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
5.4	Nástroje pro sběr logů a významných provozních událostí	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
5.5	Redundantní infrastruktura pro záložní DC pro provoz zabezpečovaného IS a bezpečnostních technologií – HW	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč

5.6	Systémový SW pro redundantní infrastrukturu pro záložní DC pro provoz zabezpečovaného IS a bezpečnostních technologií – SW	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
6	**Vysokomýtská nemocnice (NVM)**								
6.1	Rozšíření Anti-X řešení pro ochranu před škodlivým kódem	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
6.2	Nástroje pro ochranu síťového perimetru	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
6.3	Nástroje pro segmentaci sítí a řízení přístupu k síti	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
6.4	Nástroje monitorování a bezpečnost počítačových sítí	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
6.5	Řízení přístupu uživatelů a administrátorů	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
6.6	Zálohovací infrastruktura pro záložní DC pro zálohování dat a technologií zabezpečovaného IS – HW	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
6.7	Software pro zálohovací infrastrukturu pro záložní DC pro zálohování dat a technologií zabezpečovaného IS – SW	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
6.8	Nástroje pro sběr logů a významných provozních událostí	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
6.9	Infrastruktura pro provoz bezpečnostních technologií	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
6.10	Systémový SW pro provoz bezpečnostních technologií	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
7	**Rehabilitační ústav Brandýs nad Orlicí (RÚ BnO)**								
7.1	Nástroje pro ochranu síťového perimetru	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
7.2	Nástroje monitorování a bezpečnost počítačových sítí	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
7.3	Redundantní infrastruktura pro záložní DC pro provoz zabezpečovaného IS – HW	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
7.4	Systémový SW pro redundantní infrastrukturu pro záložní DC pro provoz zabezpečovaného IS – SW	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
7.5	Nástroje pro sběr logů a významných provozních událostí	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
7.6	Infrastruktura pro provoz bezpečnostních technologií	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
7.7	Systémový SW pro provoz bezpečnostních technologií	soubor	1		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
8	**Ostatní systémy a technologie**								
8.1	Nástroje pro penetrační testy a penetrační testy	ks	5		0,00 Kč	0,00 Kč		0,00 Kč	0,00 Kč
-	**Rozšíření záruky a maintenance**								
RZ	Rozšíření záruky u vybraných komponent nad 36 měsíců (37 - 60 měsíc)	soubor	1		0,00 Kč	0,00 Kč	---	---	---
RM	Rozšíření maintenance u vybraných komponent nad 36 měsíců (37 - 60 měsíc)	soubor	1		0,00 Kč	0,00 Kč	---	---	---
-	**Ostatní servisní a provozní služby**								
RP	Rozšířená podpora	hod / čtvrtletí	30		-	-	0,00 Kč	0,00 Kč	0,00 Kč
Celkem				**0,00 Kč**	**0,00 Kč**	**0,00 Kč**	**0,00 Kč**	**0,00 Kč**	**0,00 Kč**

Pokyny pro účastníka: Účastník vyplňuje jen zeleně zvýrazněné položky

Doplní dodavatel

Kritérium č. 2 - Celková kvalita nabídky (hodnoceno bude maximálně 5 zakázek u každého člena realizačního týmu dle podmínek stanovených v bodě 13 zadávací dokumentace)		
Vedoucí realizačního týmu		
1.	Název zakázky	
	Termín realizace zakázky	
	Stručný popis obsahu plnění	
	Jednalo se o zakázku v oblasti zdravotnictví	ANO / NE
	Rozsah v Kč bez DPH	
	Název objednatele	
	Kontakt na objednatele	
2.	Název zakázky	
	Termín realizace zakázky	
	Stručný popis obsahu plnění	
	Jednalo se o zakázku v oblasti zdravotnictví	ANO / NE
	Název objednatele	
	Kontakt na objednatele	
3.	Název zakázky	
	Termín realizace zakázky	
	Stručný popis obsahu plnění	
	Jednalo se o zakázku v oblasti zdravotnictví	ANO / NE
	Rozsah v Kč bez DPH	
	Název objednatele	
	Kontakt na objednatele	
4.	Název zakázky	
	Termín realizace zakázky	
	Stručný popis obsahu plnění	
	Jednalo se o zakázku v oblasti zdravotnictví	ANO / NE
	Rozsah v Kč bez DPH	
	Název objednatele	
	Kontakt na objednatele	
5.	Název zakázky	
	Termín realizace zakázky	
	Stručný popis obsahu plnění	
	Jednalo se o zakázku v oblasti zdravotnictví	ANO / NE
	Rozsah v Kč bez DPH	
	Název objednatele	
	Kontakt na objednatele	
Technický specialista – analýza bezpečnostních logů		
1.	Název zakázky	
	Termín realizace zakázky	
	Stručný popis obsahu plnění	
	Jednalo se o zakázku v oblasti zdravotnictví	ANO / NE
	Rozsah v Kč bez DPH	
	Název objednatele	

	Kontakt na objednatele	
2.	Název zakázky	
	Termín realizace zakázky	
	Stručný popis obsahu plnění	
	Jednalo se o zakázku v oblasti zdravotnictví	ANO / NE
	Rozsah v Kč bez DPH	
	Název objednatele	
	Kontakt na objednatele	
3.	Název zakázky	
	Termín realizace zakázky	
	Stručný popis obsahu plnění	
	Jednalo se o zakázku v oblasti zdravotnictví	ANO / NE
	Rozsah v Kč bez DPH	
	Název objednatele	
	Kontakt na objednatele	
4.	Název zakázky	
	Termín realizace zakázky	
	Stručný popis obsahu plnění	
	Jednalo se o zakázku v oblasti zdravotnictví	ANO / NE
	Rozsah v Kč bez DPH	
	Název objednatele	
	Kontakt na objednatele	
5.	Název zakázky	
	Termín realizace zakázky	
	Stručný popis obsahu plnění	
	Jednalo se o zakázku v oblasti zdravotnictví	ANO / NE
	Rozsah v Kč bez DPH	
	Název objednatele	
	Kontakt na objednatele	

Specialista řešení kybernetických bezpečnostních incidentů		
1.	Název zakázky	
	Termín realizace zakázky	
	Stručný popis obsahu plnění	
	Jednalo se o zakázku v oblasti zdravotnictví	ANO / NE
	Rozsah v Kč bez DPH	
	Název objednatele	
	Kontakt na objednatele	
2.	Název zakázky	
	Termín realizace zakázky	
	Stručný popis obsahu plnění	
	Jednalo se o zakázku v oblasti zdravotnictví	ANO / NE
	Rozsah v Kč bez DPH	
	Název objednatele	
	Kontakt na objednatele	
3.	Název zakázky	
	Termín realizace zakázky	
	Stručný popis obsahu plnění	
	Jednalo se o zakázku v oblasti zdravotnictví	ANO / NE
	Rozsah v Kč bez DPH	
	Název objednatele	
	Kontakt na objednatele	

4.	Název zakázky	
	Termín realizace zakázky	
	Stručný popis obsahu plnění	
	Jednalo se o zakázku v oblasti zdravotnictví	ANO / NE
	Rozsah v Kč bez DPH	
	Název objednatele	
	Kontakt na objednatele	
5.	Název zakázky	
	Termín realizace zakázky	
	Stručný popis obsahu plnění	
	Jednalo se o zakázku v oblasti zdravotnictví	ANO / NE
	Rozsah v Kč bez DPH	
	Název objednatele	
	Kontakt na objednatele	

Příloha č. 6 Zadávací dokumentace – Závazný návrh smlouvy

SMLOUVA O DODÁVCE HW A SW A O POSKYTOVÁNÍ SOUVISEJÍCÍCH SLUŽEB

na projektu Kybernetická bezpečnost poskytovatelů zdravotních služeb následné péče Pardubického kraje

uzavřená § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“)

Evidenční číslo smlouvy: [BUDE DOPLNĚNO]

Pardubický kraj

Sídlo: Komenského náměstí 125, 532 11 Pardubice I - Pardubice - Staré Město
Zastoupen: JUDr. Martin Netolický, Ph.D., hejtman
Ve věcech smluvních a převzetí plnění oprávněn/a jednat:
Ing. Pavel Špaček, e-mail:pavel.spacek@pardubickykraj.cz, tel.: 731 406 394
Ing. Kristýna Boukalová, e-mail:kristyna.boukalova@pardubickykraj.cz, tel.: 724 652 029
Ve věcech technických oprávněn/a jednat:
Ing. Pavel Špaček, e-mail:pavel.spacek@pardubickykraj.cz, tel.: 731 406 394
Ve věcech projektových oprávněn/a jednat:
Ing. Kristýna Boukalová, e-mail: kristyna.boukalova@pardubickykraj.cz, tel.: 724 652 029
IČO: 70892822
DIČ: CZ70892822
Bankovní spojení: ČSOB a.s., Pardubice, č. ú.: 220764424/0300
ID datové schránky: z28bwu9
dále jen **„Objednatel“** na straně jedné,

(na straně jedné, dále jen „**objednatel**“)

a

[DOPLNÍ DODAVATEL]

Sídlo:	[DOPLNÍ DODAVATEL]
Korespondenční adresa:	[DOPLNÍ DODAVATEL]
IČO:	[DOPLNÍ DODAVATEL]
DIČ:	[DOPLNÍ DODAVATEL]
zapsaný v obchodním rejstříku	[DOPLNÍ DODAVATEL]
zastoupený:	[DOPLNÍ DODAVATEL]
Bankovní spojení:	[DOPLNÍ DODAVATEL]
Číslo účtu:	[DOPLNÍ DODAVATEL]
Kontaktní osoba:	[DOPLNÍ DODAVATEL]
tel. kontaktní osoby:	[DOPLNÍ DODAVATEL]
e-mail:	[DOPLNÍ DODAVATEL]

(na straně druhé, dále jen „**poskytovatel**“)

(objednatel a poskytovatel dále společně také jako „**smluvní strany**“ a každá jednotlivě jako „**smluvní strana**“)

uzavírají níže uvedeného dne, měsíce a roku tuto smlouvu o servisu dodávce HW a SW a o poskytování souvisejících služeb (dále jen „**smlouva**“).

Preambule

1. Tato smlouva se uzavírá v souvislosti s realizací projektu „Kybernetická bezpečnost poskytovatelů ZS následné péče Pardubického kraje“ (dále jen „**projekt**“). Pardubický kraj je v rámci tohoto projektu příjemcem finanční podpory z Integrovaného regionálního operačního programu, č. výzvy 3 (dále jen „**Výzva 3 IROP**“), registrační číslo projektu CZ.06.01.01/00/22_003/0000043. Služby a dodávky, které jsou předmětem této smlouvy, jsou spolufinancovány z Výzvy 3 IROP a z rozpočtu Pardubického kraje. Smluvní strany této smlouvy jsou seznámeny s podmínkami stanovenými Výzvou 3 IROP, podmínkami pro účast v projektu a jsou rovněž obeznámeny s koncepcí projektu.
2. Poskytovatel je vybraným dodavatelem veřejné zakázky s názvem **„[BUDE DOPLNĚNO]“** (dále jen „**Veřejná zakázka**“) uveřejněné na profilu objednatele, jakožto zadavatele, ve smyslu zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“), zadávané v otevřeném nadlimitním řízení. Služby, které jsou předmětem této smlouvy, navazují na dodávku infrastruktury a bezpečnostních technologií dle Smlouvy o dodávce.
3. Poskytovatel prohlašuje, že je držitelem potřebného živnostenského oprávnění a má řádné vybavení, zkušenosti a schopnosti, aby dodávky a služby dle této smlouvy poskytoval ve stanovené době a ve sjednané kvalitě a že si je vědom skutečnosti, že objednatel má značný zájem na plnění předmětu této smlouvy, v čase a kvalitě stanovené touto smlouvou.

I.
Účel smlouvy

1. Účelem této smlouvy je zajištění realizace předmětu Veřejné zakázky dle zadávací dokumentace Veřejné zakázky (dále jen „**Zadávací dokumentace**“), tj. dodávky bezpečnostních technologií, HW, SW včetně licencí, implementace do stávajícího prostředí objednatele, včetně využití stávajících produktů, licencí a smluvních vztahů objednatele, záruky a rozšířené servisní podpory, a to v souladu s požadavky objednatele definovanými touto Smlouvou.
2. Poskytovatel touto smlouvou garantuje objednateli splnění zadání Veřejné zakázky a všech z toho vyplývajících podmínek a povinností podle Zadávací dokumentace. Tato garance je nadřazena ostatním podmínkám a garancím uvedeným v této Smlouvě. Pro vyloučení jakýchkoliv pochybností to znamená, že:
   a) v případě jakékoliv nejistoty ohledně výkladu ustanovení této Smlouvy budou tato ustanovení vykládána tak, aby v co nejširší míře zohledňovala účel a předmět plnění Veřejné zakázky vyjádřený Zadávací dokumentací;
   b) v případě chybějících ustanovení této smlouvy budou použita dostatečně konkrétní ustanovení Zadávací dokumentace;
   c) poskytovatel je vázán svou nabídkou předloženou objednateli v rámci zadávacího řízení na zadání Veřejné zakázky, která se pro úpravu vzájemných vztahů vyplývajících z této Smlouvy použije subsidiárně.

II.
Předmět smlouvy

1. Poskytovatel se zavazuje poskytnout objednateli plnění podrobně specifikované v přílohách č. 1 a č. 2 této Smlouvy spočívající v dodávce, instalaci a implementaci bezpečnostních technologií, HW a SW komponent včetně licencí, jakož i vzájemné funkční provázání těchto komponent a poskytnutí požadované servisní podpory, včetně dalších činností (dále jen „**Dodávka**“). Poskytovatel odevzdá věci, které jsou předmětem Dodávky, a umožní objednateli nabýt vlastnické právo k nim.
2. Poskytovatel se zavazuje poskytnout objednateli Dodávku řádně a včas za podmínek dle této smlouvy.
3. Objednatel se zavazuje zaplatit poskytovateli dohodnutou cenu za řádně a včas poskytnutou Dodávku a poskytnout poskytovateli součinnost nezbytnou k řádnému poskytnutí Dodávky, a to za podmínek touto smlouvou dále stanovených.
4. Poskytovatel se zavazuje Dodávku poskytovat sám, nebo s využitím poddodavatelů, které uvedl v příloze č. 4 této Smlouvy dle přílohy č. 6 Zadávací dokumentace a prostřednictvím osob – členů realizačního týmu, které uvedl v příloze č. 5 této Smlouvy dle přílohy č. 4 Zadávací dokumentace. Jakákoliv dodatečná změna osoby člena realizačního týmu, poddodavatele nebo rozsahu plnění svěřeného poddodavateli musí být předem písemně schválena objednatelem, ledaže by plnění původně svěřené poddodavateli realizoval poskytovatel sám. Nový člen realizačního týmu musí odpovídat požadavkům stanoveným objednatelem v Zadávací dokumentaci.
5. Smluvní strany výslovně uvádějí, že při poskytování Dodávky prostřednictvím poddodavatele má poskytovatel odpovědnost, jako by Dodávku poskytoval sám. Objednatel bude jednat vždy výhradně s poskytovatelem.

III.
Termíny a místo plnění

1. Nevyplývá-li z této Smlouvy výslovně jinak, je poskytovatel povinen provést Dodávku nejpozději do 280 kalendářních dnů od nabytí účinnosti této Smlouvy, dle harmonogramu uvedeného v příloze č. 1 a poskytovat záruku a servisní podporu po dobu 5 let dle přílohy č. 2 této Smlouvy. Tím není dotčeno ustanovení čl. V. odst. 12 smlouvy.
2. Místa plnění této veřejné zakázky jsou uvedena v přílohách č. 1 a č. 2 této Smlouvy. Pokud to povaha plnění dle smlouvy umožňuje, je poskytovatel oprávněn poskytovat plnění dle smlouvy také vzdáleným přístupem.

IV.
Způsob provedení dodávky

1. V rámci Dodávky je poskytovatel povinen provést instalaci a zprovoznění jednotlivých bezpečnostních technologií, HW a SW komponent tvořících Dodávku, jakož i vzájemné funkční provázání těchto komponent a poskytnutí požadované servisní podpory, včetně dalších činností, a to v souladu s **přílohami č. 1 a č. 2** této Smlouvy.

2. V rámci provedení Dodávky a v rámci poskytnutí Licencí k autorským dílům tvořícím součást Dodávky je poskytovatel povinen předat objednateli veškerou dokumentaci, doklady, záruční listy, technické a uživatelské manuály a jiné dokumenty, které jsou nezbytné k řádnému užívání komponent tvořících Dodávku, jakož i k užívání Dodávky jako celku. Předáním dokumentace je myšleno zejména dodání následujících dokumentů: licenční podmínky k autorským dílům, která jsou standardním produktem dle odst. 5 tohoto článku smlouvy, uživatelské manuály, detailní přehled veškerého instalovaného zařízení a komponent, konfigurace dodaných technologií a systémů, seznam IP adres a použití, seznam rozšíření (Extension list) a další projektová dokumentace (dále jen „**Dokumentace**“).
3. Objednatel akceptuje provedení Dodávky na základě provedené akceptační procedury dle ustanovení čl. V. této smlouvy.
4. Dodávka HW a SW včetně licencí je řádně provedena okamžikem podpisu akceptačního protokolu dle čl. V. odst. 4 smlouvy ze strany objednatele. Tímto okamžikem přechází na objednatele vlastnické právo a nebezpečí škody způsobené na věcech tvořících součást Dodávky.
5. Pokud je součástí Dodávky poskytovatele poskytnutí doplňkového programového vybavení (software, systémové komponenty) nebo jiného předmětu (např. Dokumentace), který naplňuje znaky díla dle zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „**autorské dílo**“), zavazuje se poskytovatel objednateli poskytnout nebo zajistit pro objednatele oprávnění užít veškerá takováto autorská díla všemi v úvahu přicházejícími způsoby užití nezbytnými k řádnému užívání Dodávky objednatelem po dobu trvání majetkových práv autorských autora k autorskému dílu, bez jakýchkoliv množstevních nebo územních omezení (dále jen „**Licence**“). V případě, že autorské dílo je standardním komerčním softwarovým produktem poskytovatele nebo třetí strany, objednatel připouští omezení Licence v nezbytném rozsahu z této skutečnosti vyplývajícího, umožňujícího naplnění předmětu a účelu této smlouvy. Smluvní strany se výslovně dohodly, že veškeré předmětné Licence budou objednateli poskytnuty bez nároku na dodatečnou odměnu nad rámec ceny Dodávky sjednané v této smlouvě a náklady na pořízení příslušné Licence jsou součástí ceny Dodávky dle této smlouvy.
6. Poskytovatel se zavazuje zajistit platnost Licencí k autorským dílům třetích stran a možnost objednatele užít veškerá takováto autorská díla v souladu s předmětem této smlouvy a k účelům vyplývajícím z této smlouvy.
7. Poskytovatel prohlašuje, že veškeré jeho plnění dodané podle této smlouvy bude prosté právních vad a zavazuje se odškodnit v plné výši objednatele v případě, že třetí osoba úspěšně uplatní autorskoprávní nebo jiný nárok plynoucí z právní vady poskytnutého plnění. V případě, že by nárok třetí osoby vzniklý v souvislosti s plněním poskytovatele podle této smlouvy, bez ohledu na jeho oprávněnost, vedl k dočasnému či trvalému soudnímu (či obdobnému) zákazu či omezení užívání Dodávky či jeho části ze strany objednatele, zavazuje se poskytovatel zajistit náhradní řešení a minimalizovat dopady takovéto situace na objednatele, a to bez dopadu na cenu Dodávky sjednanou podle této smlouvy, přičemž současně nebudou dotčeny ani nároky objednatele na náhradu škody.

V.
Akceptace

1. Část Dodávky, tvořící logický a funkční celek způsobilý být předmětem přejímky (dále jen „**dílčí plnění**“), bude objednatelem akceptována na základě akceptační procedury. Akceptační procedura zahrnuje ověření, zda poskytovatelem poskytnuté dílčí plnění splňuje podmínky, k jejichž splnění se poskytovatel zavázal, a to porovnáním skutečných vlastností jednotlivých dílčích plnění poskytovatele s jejich závaznou specifikací uvedenou v této smlouvě; specifikací se rozumí i akceptační kritéria, jsou-li stanovena dohodou Smluvních stran.
2. Předání a převzetí poskytovatelem řádně provedené Dodávky, která je samostatným dílčím plněním, proběhne na základě níže popsané akceptační procedury, a to v termínu dle čl. III. odst. 1 této smlouvy.
3. Poskytovatel písemně vyzve objednatele k účasti na akceptační proceduře nejméně 7 pracovních dnů před jejím zahájením. Pokud se objednatel nedostaví v termínu určeném pro provedení akceptačních testů, přestože byl poskytovatelem k účasti řádně vyzván, je poskytovatel oprávněn provést příslušné akceptační testy bez jeho přítomnosti. O průběhu akceptačních testů vyhotoví poskytovatel písemný záznam, v němž zejména uvede, zda testy prokázaly chyby. Objednateli budou poskytnuty originály veškerých dokumentů vypracovaných v souvislosti s provedením akceptačních testů.
4. Jestliže jednotlivé dílčí plnění splní akceptační kritéria akceptačních testů, poskytovatel se zavazuje nejpozději v pracovní den následující po ukončení akceptačních testů umožnit objednateli toto dílčí plnění převzít a objednatel se zavazuje k jeho převzetí nejpozději do 5 pracovních dnů. Smluvní strany se zavazují o tomto převzetí sepsat akceptační protokol, jehož vzor je přílohou č. 6 této smlouvy.
5. Nestanoví-li specifikace akceptačních testů jinak, má se za to, že dílčí plnění splňuje stanovená akceptační kritéria za předpokladu, že toto plnění nemá žádnou vadu kategorie A ve smyslu odst. 6 tohoto článku smlouvy, a současně nemá více než 2 vady kategorie B ve smyslu odst. 7 tohoto článku smlouvy – v takovém případě objednatel může podepsat akceptační protokol s výrokem „Akceptováno s výhradami“. V případech, kdy počet a/nebo druh vad překračuje maximální počet stanovený pro splnění akceptačních kritérií s výrokem „Akceptováno s výhradami“, objednatel uvede do akceptačního protokolu výrok „Neakceptováno“ a není povinen Dodávku či dílčí plnění převzít.
6. Vadou kategorie A je vada, která zcela nebo podstatným způsobem znemožňuje použití dílčího plnění pro potřeby objednatele v souladu s touto smlouvou.
7. Vadou kategorie B je vada, která umožňuje použití dílčího plnění pro potřeby objednatele v souladu s touto smlouvou, ovšem dílčí plnění neodpovídá jeho specifikaci dle této smlouvy.
8. Za úspěšnou se akceptační procedura považuje v okamžiku, kdy je oběma stranami podepsán akceptační protokol s výrokem „Akceptováno bez výhrad“.
9. Pokud kterékoliv z jednotlivých dílčích plnění nesplňuje stanovená akceptační kritéria nebo je splňuje s vadami, které jsou přípustné, sdělí objednatel své připomínky písemně poskytovateli; pokud objednatel takové dílčí plnění současně akceptuje, uvede své připomínky v akceptačním protokolu.

10. Poskytovatel je povinen vypořádat připomínky objednatele bez zbytečného odkladu a neprodleně předložit příslušné dílčí plnění k opakované akceptaci dle této smlouvy, za přiměřeného použití ostatních ustanovení tohoto článku smlouvy. Akceptační procedura se bude opakovat, dokud příslušné dílčí plnění nesplní akceptační kritéria a nebude možné zakončit akceptaci s výrokem „Akceptováno bez výhrad“. V případě, že se jedná o vypořádání připomínek k dílčímu plnění, které již bylo akceptováno, namísto akceptačního protokolu strany potvrdí písemně, že připomínky byly vypořádány.

11. Dohodnuté termíny pro akceptaci dílčího plnění nejsou dotčeny trváním akceptační procedury ani jakýmkoli jejím prodloužením z důvodu vad bránících akceptaci, tj. pokud akceptační procedura z důvodů na straně poskytovatele či z důvodů jejího nutného opakování ve smyslu odst. 9 tohoto článku smlouvy či jiných vad bránících akceptaci překročí termín uvedený v čl. III. odst. 1 této smlouvy, bude se jednat o prodlení poskytovatele s plněním Dodávky.

12. V souladu s čl. IV. odst. 5 smlouvy je poskytovatel povinen poskytnout objednateli veškeré Licence k autorským dílům tvořícím součást Dodávky (či s touto Dodávkou souvisejících) nejpozději v den podpisu akceptačního protokolu Dodávky. Přede dnem podpisu akceptačního protokolu Dodávky je objednatel oprávněn užívat autorská díla dle předešlé věty v rozsahu nezbytně nutném k provedení akceptační procedury dle tohoto článku smlouvy a k ověření kvality plnění poskytovatele.

13. Není-li touto smlouvou stanoveno jinak, je poskytovatel nejpozději v den podpisu akceptačního protokolu jednotlivého dílčího plnění povinen předat objednateli Dokumentaci, včetně provozní, uživatelské a administrátorské dokumentace k dílčímu plnění.

VI.
Cena a platební podmínky

1. Cena za plnění dle této smlouvy (za dodávku i servisní služby) je cenou smluvní, nejvýše přípustnou, nepřekročitelnou a maximálně činí [BUDE DOPLNĚNO] bez DPH, samostatně DPH ve výši [BUDE DOPLNĚNO], tj. celkem [BUDE DOPLNĚNO] včetně DPH. Z toho:

    a. cena za dodávku činí: [BUDE DOPLNĚNO] bez DPH, samostatně DPH ve výši [BUDE DOPLNĚNO], tj. celkem [BUDE DOPLNĚNO] včetně DPH.
    b. cena za servisní služby za 1 kalendářní čtvrtletí činí: [BUDE DOPLNĚNO] bez DPH, samostatně DPH ve výši [BUDE DOPLNĚNO], tj. celkem [BUDE DOPLNĚNO] včetně DPH

    Detailní rozpad ceny za plnění je uveden v příloze č. 3 této smlouvy.

2. Cena za Dodávku dle přílohy č. 1 této Smlouvy zahrnuje veškeré náklady poskytovatele spojené s Dodávkou a zahrnují zejména veškeré Licence vztahující se k či související s příslušnou částí Dodávky, základní záruku a servisní činnost po dobu 3 let ode dne akceptace s výrokem „Akceptováno bez výhrad“, a dále veškeré služby, které budou poskytovatelem k Dodávce či v souvislosti s Dodávkou poskytovány. Cenu je možné změnit pouze v případě změny sazby DPH. Poskytovatel prohlašuje, že všechny technické, finanční, věcné a ostatní podmínky pro splnění závazků z této smlouvy zahrnul do kalkulace ceny. Poskytovatel výslovně prohlašuje, že součástí ceny jsou i veškeré náklady spojené se splněním podmínek pro splnění závazků z této smlouvy dle obecně závazných právních předpisů.

3. Cena za servisní služby dle této smlouvy, zejména přílohy č. 2 této smlouvy, je cenou smluvní, nejvýše přípustnou, nepřekročitelnou. Cena za servisní služby zahrnuje veškeré náklady poskytovatele spojené se splněním jeho závazku z této smlouvy, zejména přílohy č. 2. Cenu je možné změnit (s výjimkou odst. 4 tohoto článku smlouvy) pouze v případě změny sazby DPH. Poskytovatel prohlašuje, že všechny technické, finanční, věcné a ostatní podmínky pro splnění závazků z této smlouvy zahrnul do kalkulace ceny. Poskytovatel výslovně prohlašuje, že součástí ceny jsou i veškeré náklady spojené se splněním podmínek pro splnění závazků z této smlouvy dle obecně závazných právních předpisů.
4. Vícepráce i vícenáklady, které vzniknou poskytovateli z důvodu poskytnutí nekvalitních služeb či služeb poskytnutých v rozporu se smlouvou či jejími přílohami, nejsou součástí ceny a hradí je poskytovatel v plné výši.
5. Cena zahrnuje veškeré činnosti poskytovatele a požadavky objednatele, uvedené v přílohách č. 1 a č. 2 smlouvy.
6. Objednatel nebude poskytovat žádné zálohové platby.
7. Úhrada ceny bude provedena po poskytnutí služeb v české měně nebo v měně platné v České republice na základě řádného daňového dokladu (dále jen jako „**faktura**“), kterou je poskytovatel povinen vystavit nejpozději do 10. kalendářního dne ode dne akceptace/převzetí dodávek nebo služeb. Datem uskutečnění zdanitelného plnění je datum akceptace/převzetí dodávek nebo služeb. Splatnost faktury je smluvními stranami dohodnuta na 30 (třicet) kalendářních dnů ode dne řádného doručení faktury objednateli.
8. Podkladem a podmínkou pro vystavení řádné faktury za Dodávku dle odst. 1 tohoto článku smlouvy bude objednatelem podepsaný akceptační protokol s výrokem „Akceptováno bez výhrad“ a musí obsahovat minimálně název projektu, registrační číslo projektu a informaci o tom, že Projekt je spolufinancován z Integrovaného operačního programu (IROP) včetně povinných parametrů publicity. Tento akceptační protokol bude přílohou faktury.
9. Podkladem a podmínkou pro vystavení řádné faktury za servisní služby dle odst. 2 tohoto článku smlouvy bude objednatelem potvrzený report příslušného kalendářního čtvrtletí, který bude ze strany poskytovatele předáván čtvrtletně, vždy za celé ukončené jednotlivé kalendářní čtvrtletí zpětně k posledními dni čtvrtletí, a musí obsahovat minimálně název projektu, registrační číslo projektu, informaci o tom, že Projekt je spolufinancován z Integrovaného regionálního operačního programu (IROP) včetně povinných parametrů publicity, číslo reportu, období, datum činnosti, konkrétní popis činnosti, identifikační údaje poskytovatele a dále výpis všech záznamů Hotline a Helpdesk z dotčeného čtvrtletí a jejich stav vyřízení poskytovatelem, souhrnné informace ohledně dodržování garance provozu (SLA) za dotčený kalendářní čtvrtletí. Tento report bude přílohou faktury.
10. V případě, že budou služby poskytovány jen po část kalendářního čtvrtletí, bude poměrně zkrácena příslušná fakturace za poskytování služeb.
11. Stane-li se v průběhu trvání smlouvy Česká republika členem Evropské měnové unie a bude-li v závazně stanoven koeficient pro přepočet CZK na EUR, budou ceny sjednané v CZK přepočteny do EUR na základě odpovídajícího koeficientu sjednaného v mezinárodních úmluvách, kterými bude Česká republika vázána, jakož i v souladu s případnou tomu odpovídající vnitrostátní právní úpravou České republiky.
12. Faktury vystavené poskytovatelem musí obsahovat všechny náležitosti daňového dokladu dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „**zákon o DPH**“), a dle § 435 občanského zákoníku vč. označení smlouvy, ke které se

vztahuje. Faktura bude dále obsahovat náležitosti vyplývající z režimu spolufinancování Projektu z Evropské unie, zejména registrační číslo projektu CZ.06.01.01/00/22_003/0000043, název projektu „Kybernetická bezpečnost poskytovatelů zdravotních služeb následné péče Pardubického kraje“ a informaci o tom, že Projekt je spolufinancován z Integrovaného regionální operačního programu (IROP) včetně povinných parametrů publicity, dále cenu bez DPH, sazbu DPH a cenu vč. DPH.

13. Nebude-li faktura obsahovat veškeré náležitosti podle zákona o DPH, občanského zákoníku nebo podle jiných obecně platných právních předpisů nebo bude-li v rozporu s podmínkami stanovenými smlouvou, nebo bude-li chybně vyúčtována cena nebo DPH, je objednatel oprávněn fakturu poskytovateli vrátit s pokyny k její opravě. V takovém případě splatnost faktury nezačala běžet a splatnost nové opravné faktury počne běžet od samého počátku až prvním dnem po jejím doručení objednateli.
14. Povinnost uhradit cenu za poskytnuté služby je splněna dnem odepsání příslušné částky z účtu objednatele ve prospěch účtu poskytovatele. Všechny poukazované částky vzájemně stranami na základě smlouvy musí být prosté jakýchkoliv bankovních poplatků nebo jiných nákladů spojených s převodem na jejich účty.
15. Objednatel uhradí přijatou fakturu pouze na bankovní účty poskytovatele zveřejněné správcem daně způsobem umožňujícím dálkový přístup ve smyslu § 96 odst. 2 zákona o DPH. V případě, že poskytovatel nebude mít svůj bankovní účet tímto způsobem zveřejněn, uhradí objednatel poskytovateli pouze základ daně, přičemž DPH uhradí poskytovateli až po zveřejnění příslušného účtu poskytovatele v registru plátců a identifikovaných osob poskytovatelem.
16. Poskytovatel prohlašuje, že správce daně před uzavřením smlouvy nerozhodl, že poskytovatel je nespolehlivým plátcem ve smyslu § 106a zákona o DPH (dále jen „nespolehlivý plátce“). V případě, že správce daně rozhodne o tom, že poskytovatel je nespolehlivým plátcem, zavazuje se poskytovatel o tomto informovat objednatele do 2 (slovy: dvou) pracovních dní. Stane-li se poskytovatel nespolehlivým plátcem nebo dojde k některé ze skutečností předvídaných v § 109 zákona o DPH, uhradí objednatel poskytovateli pouze základ daně, přičemž DPH je objednatel oprávněn uhradit přímo příslušnému správci daně, přičemž tato úhrada se považuje za řádné splnění povinnosti zaplatit cenu dle smlouvy. O úhradě DPH přímo příslušnému správci daně je objednatel povinen poskytovatele písemně informovat.

VII.
Práva a povinnosti stran, prohlášení stran

1. Poskytovatel se zavazuje:
   a) poskytovat Dodávku podle této smlouvy a servisní služby a záruky vlastním jménem, na vlastní odpovědnost a v souladu s pokyny objednatele řádně a včas, zejména se zohledněním délky trvání akceptační procedury;
   b) poskytovat Dodávku dle této smlouvy výhradně s využitím nového, nerepasovaného zboží, které pochází z oficiálního distribučního kanálu výrobce dodávaného zařízení a je určeno pro trh v České republice;
   c) poskytovat Dodávku dle této smlouvy spočívající v instalaci a veškeré konzultační, servisní či obdobné činnost vztahující se k dodanému HW či SW členy realizačního týmu, které uvedl v příloze č. 5 této Smlouvy;

d) poskytovat plnění podle této smlouvy s péčí řádného hospodáře odpovídající podmínkám sjednaným v této smlouvě a s procesy „best practice“;
e) upozorňovat objednatel včas na všechny hrozící vady či výpadky svého plnění, jakož i poskytovat objednateli veškeré informace, které jsou pro plnění smlouvy nezbytné;
f) neprodleně oznámit písemnou formou objednateli překážky, které mu brání v plnění předmětu smlouvy a výkonu dalších činností souvisejících s plněním předmětu smlouvy;
g) upozornit objednatele na potenciální rizika vzniku škod a včas a řádně dle svých možností provést taková opatření, která riziko vzniku škod zcela vyloučí nebo sníží;
h) informovat objednatele o plnění svých povinností podle této smlouvy a o důležitých skutečnostech, které mohou mít vliv na výkon práv a plnění povinností smluvních stran;
i) zajistit, aby všechny osoby podílející se na plnění jeho závazků z této Smlouvy, které se budou zdržovat v prostorách nebo na pracovištích objednatele, dodržovaly účinné právní předpisy o bezpečnosti a ochraně zdraví při práci a veškeré interní předpisy objednatele, s nimiž objednatel poskytovatele obeznámil;
j) chránit osobní údaje, data a duševní vlastnictví objednatele a třetích osob;
k) upozorňovat objednatele v odůvodněných případech na případnou nevhodnost pokynů objednatele.

2. Poskytovatel prohlašuje, že:

a) není jako právnická osoba v likvidaci;
b) není proti němu vedeno konkursní řízení ani vyrovnací řízení ve smyslu zákona č. 328/1991 Sb., o konkursu a vyrovnání, ve znění pozdějších předpisů, popř. zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení, ve znění pozdějších předpisů a takové řízení nebylo zastaveno či zrušeno z důvodu nedostatku majetku poskytovatele a dále není předlužen či neschopen plnit své splatné závazky vůči svým věřitelům;
c) uzavření/m této smlouvy:

- neporuší správní rozhodnutí orgánu státní správy České republiky či rozhodnutí soudů České republiky;
- neporuší ustanovení žádné dohody, smlouvy či jiného ujednání, které uzavřel se třetí osobou;
- neučinil nic, ať již sám anebo za spolupráce či prostřednictvím třetí osoby, co by omezilo či znemožnilo dosažení účelu této smlouvy.

3. Poskytovatel se zavazuje, že objednateli bezodkladně po vzniku takové skutečnosti písemně oznámí:

a) podání návrhu na prohlášení konkursu na majetek poskytovatele dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení, ve znění pozdějších předpisů; nebo
b) podání návrhu na vyrovnání na majetek poskytovatele dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení, ve znění pozdějších předpisů; nebo
c) vstup poskytovatele do likvidace; nebo
d) splnění podmínek prohlášení konkursu na majetek poskytovatele, tj. zejména že poskytovatel je předlužen anebo insolventní; nebo

e) rozhodnutí o provedení přeměny poskytovatele, zejména fúzí, převodem jmění na společníka či rozdělením, provedení změny právní formy poskytovatele či provedení jiných organizačních změn; nebo

f) omezení či ukončení činnosti poskytovatele, která bezprostředně souvisí s předmětem této smlouvy; nebo

g) všechny skutečnosti, které by mohly mít vliv na přechod či vypořádání závazků poskytovatele vůči objednateli vyplývajících z této smlouvy či s touto smlouvou souvisejících; nebo

h) rozhodnutí o zrušení poskytovatele.

4. Poskytovatel prohlašuje, že před podpisem této smlouvy řádně překontroloval veškeré podklady a dokumentaci a řádně prověřil místní podmínky a všechny nejasné podmínky pro poskytování služeb si vyjasnil s objednatelem nebo místním šetřením.

5. Poskytovatel se zavazuje mít po celou dobu trvání smluvního vztahu sjednané pojištění odpovědnosti za škodu způsobenou třetí osobě s limitním plněním na jednu škodnou událost v minimální výši [BUDE DOPLNĚNO],- Kč.

6. Poskytovatel je povinen spolupůsobit při výkonu finanční kontroly ve smyslu § 2 písm. e) a § 13 zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonu (dále jen „zákon o finanční kontrole“), ve znění pozdějších předpisů, tj. poskytnout kontrolnímu orgánu doklady o dodávkách zboží a služeb hrazených z veřejných výdajů nebo z veřejné finanční podpory v rozsahu nezbytném pro ověření příslušné operace. Tutéž povinnost bude poskytovatel povinen požadovat po svých dodavatelích.

7. Poskytovatel je povinen archivovat originální vyhotovení smlouvy včetně jejích dodatků, originály účetních dokladů (a jejich příloh) a dalších dokladů vztahujících se k realizaci předmětu této smlouvy po dobu 10 let od ukončení projektu, minimálně však do 31. 12. 2030. Po tuto dobu je poskytovatel povinen umožnit osobám oprávněným k výkonu kontroly projektů provést kontrolu dokladů souvisejících s plněním této smlouvy.

8. Veškeré materiály vztahující se k projektu (dokumenty, smlouvy, prezenční listiny, publikace, prezentace atd.), nebo vzniklé v rámci projektu musí být označeny v souladu s Obecnými a/nebo Specifickými pravidly IROP. Vedle toho objednatel požaduje, aby povinná publicita všech materiálů, které vzniknou v rámci plnění projektu, byla vždy předem odsouhlasena určeným zaměstnancem objednatele jako realizátora projektu.

VIII.
Ochrana informací, osobních údajů a bezpečnost informací

1. Smluvní strany jsou si vědomy toho, že v rámci plnění této smlouvy:

   a) si mohou vzájemně úmyslně nebo i opominutím poskytnout informace, které budou považovány za důvěrné (dále „**důvěrné informace**“),

   b) mohou jejich zaměstnanci získat vědomou činností druhé strany nebo i jejím opominutím přístup k důvěrným informacím druhé strany.

2. Veškeré důvěrné informace zůstávají výhradním vlastnictvím předávající strany a přijímající strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní důvěrné informace. S výjimkou plnění této smlouvy se obě strany zavazují neduplikovat žádným způsobem důvěrné informace druhé strany, nepředat je třetí straně ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi

potřebují být seznámeni, aby mohli plnit tuto smlouvu. Obě strany se zároveň zavazují nepoužít důvěrné informace druhé strany jinak než za účelem plnění této smlouvy.

3. Nedohodnou-li se smluvní strany výslovně jinak, považují se za důvěrné implicitně všechny informace, které jsou a nebo by mohly být součástí obchodního tajemství, tj. např. popisy nebo části popisů technologických procesů a vzorců, technických vzorců a technického know-how, informace o provozních metodách, procedurách a pracovních postupech, obchodní nebo marketingové plány, koncepce a strategie nebo jejich části, nabídky, kontrakty, smlouvy, dohody nebo jiná ujednání s třetími stranami, informace o výsledcích hospodaření, o vztazích s obchodními partnery, o pracovněprávních otázkách a všechny další informace, jejichž zveřejnění přijímající stranou by předávající straně mohlo způsobit škodu.
4. Pokud jsou důvěrné informace poskytovány v písemné podobě nebo ve formě textových souborů na počítačových médiích, je předávající strana povinna upozornit přijímající stranu na důvěrnost takového materiálu jejím vyznačením alespoň na titulní stránce.
5. Bez ohledu na výše uvedená ustanovení se za důvěrné nepovažují informace, které:
   a) se staly veřejně známými, aniž by to zavinila záměrně či opominutím přijímající strana,
   b) měla přijímající strana legálně k dispozici před uzavřením této smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi smluvními stranami uzavřené smlouvy o ochraně informací,
   c) jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je to schopna doložit svými záznamy nebo důvěrnými informacemi třetí strany,
   d) po podpisu této smlouvy poskytne přijímající straně třetí osoba, jež takové informace přitom nezíská přímo ani nepřímo od strany, jež je jejich vlastníkem.
6. Poskytovatel je povinen při poskytování plnění podle této smlouvy dodržovat zásady bezpečnosti informací a dat včetně osobních údajů (dále v tomto odstavci jen „bezpečnost informací“), jakož i zásady ochrany osobních údajů stanovených GDPR, přičemž bezpečností informací se rozumí zajišťování důvěrnosti, integrity a dostupnosti informací, které jsou uchovávány, vytvářeny nebo zpracovávány prostřednictvím prvků KI, a to v přiměřeném rozsahu.
7. Poskytovatel je povinen při plnění svých povinností podle této smlouvy s odbornou péčí poskytovat objednateli veškerou součinnost nezbytnou k tomu, aby objednatel řádně naplňoval právní povinnosti stanovené zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „ZoKB“), a jeho prováděcími předpisy. Poskytovatel je zejména povinen poskytovat objednateli součinnost k zavádění, provádění, revidování a aktualizaci odpovídajících bezpečnostních opatření stanovených objednatelem za účelem zajištění souladu se ZoKB a jeho prováděcími předpisy. Jestliže vznikne v souvislosti s povinnostmi podle tohoto odstavce potřeba uzavřít dodatek k této smlouvě nebo zvláštní smlouvu, zavazuje se poskytovatel poskytnout objednateli veškerou součinnost nezbytnou k formulaci obsahu takového dodatku, resp. smlouvy, a k uzavření takového dodatku, resp. smlouvy v souladu se ZZVZ.
8. Ustanovení tohoto článku není dotčeno ukončením této smlouvy z jakéhokoliv důvodu po dobu dalších 5 let.

IX.

Součinnost a vzájemná komunikace

1. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků vyplývajících ze smlouvy. Smluvní strany jsou povinny informovat druhou smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této Smlouvy.
2. Smluvní strany jsou povinny plnit své závazky vyplývající z této smlouvy tak, aby nedocházelo k prodlení s plněním jednotlivých termínů a s prodlením splatnosti jednotlivých peněžních závazků.
3. Veškerá komunikace mezi smluvními stranami bude probíhat prostřednictvím oprávněných osob, které si smluvní strany za tímto účelem sdělí, statutárních orgánů smluvních stran, popř. jimi písemně pověřených pracovníků.

X.
Záruka

1. Poskytovatel poskytuje záruku (včetně záruky výrobce na dodaný HW), že každá část Dodávky má ke dni její akceptace funkční vlastnosti stanovené touto smlouvou, a je způsobilá k použití pro účely stanovené v této smlouvě nebo v souladu s touto smlouvou.
2. Poskytovatel poskytuje záruku každé jednotlivé části Dodávky od okamžiku její akceptace s výrokem „Akceptováno bez výhrad“ po dobu uvedenou v příloze č. 1 této Smlouvy.
3. Objednatel je oprávněn vady Dodávky nahlásit poskytovateli kdykoli v průběhu záruční doby (základní či rozšířené) bez ohledu na to, kdy je zjistil, aniž by tím byla jeho práva ze záruky či práva z vad jakkoli dotčena.
4. Doba od zjištění vady do jejího odstranění se do trvání záruční doby nezapočítává.
5. Podrobnosti požadované základní záruky a rozšířené záruky jsou uvedeny v příloze č. 1 smlouvy.

XI.
Sankce

1. V případě prodlení poskytovatele s předáním Dodávky a s poskytnutím Licencí v termínu dle čl. III. odst. 1 smlouvy vzniká objednateli nárok na zaplacení smluvní pokuty ve výši 50.000,- Kč za každý i započatý den prodlení.
2. V případě prodlení poskytovatele s dodržením garantovaných reakčních dob (dob opravy) dle SLA k jednotlivým službám servisních služeb dle Přílohy č. 2 této smlouvy vzniká objednateli nárok na zaplacení smluvní pokuty ve výši 10.000,- Kč za každou i započatou hodinu prodlení s takovým plněním, je-li garantovaná reakční doba (doba opravy) stanovena v hodinách.
3. V případě prodlení poskytovatele s dodržením garantovaných reakčních dob (dob opravy) dle SLA k jednotlivým službám servisních služeb dle Přílohy č. 2 této Smlouvy vzniká objednateli nárok na zaplacení smluvní pokuty ve výši 10.000,- Kč za každý i započatý den prodlení s takovým plněním, je-li garantovaná reakční doba (doba opravy) stanovena ve dnech (např. úroveň 24x7 NBD – Next Business Day).
4. V případě, že poskytovatel bude k poskytování Dodávky využívat členy realizačního týmu nebo poddodavatele v rozporu s ustanoveními čl. II. odst. 4 této smlouvy, vzniká objednateli

nárok na zaplacení smluvní pokuty ve výši 50.000,- Kč za každý jednotlivý případ takového porušení smlouvy.

5. V případě, že poskytovatel poruší svou povinnost čl. VII. odst. 1 písm. b) smlouvy poskytovat Dodávku dle této Smlouvy výhradně s využitím nového, nerepasovaného zboží, které pochází z oficiálního distribučního kanálu výrobce dodávaného zařízení a je určeno pro trh v České republice, vzniká objednateli nárok na zaplacení smluvní pokuty ve výši 10.000,- Kč za každý komponent tvořící součást Dodávky, který nesplňuje uvedené podmínky.
6. V případě, že poskytovatel poruší svou povinnost dle čl. VII. odst. 1 písm. b) smlouvy poskytovat Dodávku dle této Smlouvy technickým partnerem pro servery, disková pole a síťovou infrastrukturu v České republice, který je oprávněn k provádění servisních zásahů na území České republiky, vzniká objednateli nárok na zaplacení smluvní pokuty ve výši 10.000,- Kč za každý jednotlivý případ porušení této povinnosti poskytovatele.
7. V případě, že objednatel je v prodlení s úhradou ceny za Dodávku nebo ceny za servisní služby, je povinen uhradit poskytovateli úrok z prodlení v zákonné výši, a to z dlužné částky.
8. Smluvní pokuty a úrok z prodlení jsou splatné do 30 dnů od doručení jejich vyúčtování oprávněnou smluvní stranou straně povinné. Platby budou provedeny bezhotovostním bankovním převodem na účet oprávněné smluvní strany.
9. Ustanovením o smluvní pokutě není dotčeno právo oprávněné strany na náhradu škody v plné výši. Pokud není v ostatních ustanoveních smlouvy uvedeno jinak, zaplacení smluvní pokuty poskytovatelem objednateli nezbavuje poskytovatele závazku splnit povinnosti dané mu smlouvou.
10. Každá ze stran smlouvy nese odpovědnost za prodlení, za vady a způsobenou škodu plynoucí z porušení smlouvy a obecně závazných právních předpisů, zejména občanského zákoníku. Žádná ze stran smlouvy nebude odpovědná za škodu způsobenou v důsledku okolností vylučujících odpovědnost ve smyslu občanského zákoníku. Smluvní strany se zavazují upozornit druhou stranu bez zbytečného odkladu na jakékoliv okolnosti bránící řádnému plnění smlouvy a zavazují se k maximálnímu úsilí k jejich odvrácení a překonání.

XII.
Platnost a účinnost smlouvy, její ukončení

1. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem jejího uveřejnění v registru smluv a uzavírá se na dobu určitou potřebnou pro splnění všech povinností dle této smlouvy. Ukončením této smlouvy nejsou dotčena ustanovení smlouvy týkající se převodu vlastnického práva, nároků z odpovědnosti za vady, nároků plynoucích ze záruky, nároků z odpovědnosti za škodu a nároků ze smluvních pokut, ustanovení o ochraně informací, ani další ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po zániku účinnosti této smlouvy.
2. Objednatel je oprávněn od smlouvy odstoupit zejména v případě podstatného porušení smluvní nebo zákonné povinnosti poskytovatelem.
3. Za podstatné porušení povinnosti se považuje zejména:
   a) prodlení poskytovatele s předáním jakéhokoliv dílčího plnění po dobu delší než 10 dnů oproti termínu plnění stanovenému ve smlouvě nebo na základě této smlouvy;

b) opakované nedodržení alespoň jednoho ze sledovaných parametrů SLA u Služeb, přičemž nedodržení se považuje za opakované, pokud za posledních 6 měsíců nastalo alespoň dvakrát;

c) opakované případy využívání členů realizačního týmu nebo poddodavatelů poskytovatelem v rozporu s ustanovením čl. II. odst. 4 smlouvy, přičemž za opakované se považuje, pokud za posledních 3 měsíce nastalo alespoň dvakrát;

d) vyjde najevo, že poskytovatel není z jakéhokoliv důvodu neležícího na straně objednatele schopen plnit dál své závazky z této smlouvy.;

e) jestliže bude poskytovatelem podán návrh na prohlášení konkursu na vlastní majetek ve smyslu ustanovení zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení, ve znění pozdějších předpisů nebo bude prohlášen konkurs na majetek poskytovatele na základě návrhu věřitele poskytovatele či bude na základě rozhodnutí soudu ustanoven předběžný správce konkursní podstaty pro poskytovatele ve smyslu zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení, ve znění pozdějších právních předpisů nebo bude poskytovatelem podán návrh na vyrovnání ve smyslu ustanovení zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení, ve znění pozdějších předpisů,

f) případ, kdy se prohlášení poskytovatele uvedené v příloze č. 5 zadávací dokumentace na veřejnou zakázku uvedenou v odst. 2 preambule smlouvy ukáže jako nepravdivé, a to kdykoliv po dobu trvání této smlouvy, nebo

g) poskytovatel vstoupil do likvidace.

4. Každá smluvní strana je oprávněna odstoupit od smlouvy též v případě prodlení druhé strany s plněním závazků podle této smlouvy po dobu delší než třicet (30) dnů, pokud druhá smluvní strana nezjedná nápravu ani v dodatečné přiměřené lhůtě, která jí byla smluvní stranou poskytnuta na základě písemné výzvy ke splnění povinnosti, přičemž tato lhůta nesmí být kratší než patnáct (15) dnů od doručení takovéto výzvy.

5. Účinky odstoupení od smlouvy nastávají dnem doručení písemného oznámení o odstoupení druhé smluvní straně.

6. V případě odstoupení od smlouvy má objednatel právo rozhodnout, zda si rozpracované plnění ponechá. Rozpracovaným plněním se myslí Dodávka jako celek až do okamžiku jejího řádného převzetí objednatelem. V případě, že si objednatel rozpracované plnění ponechá, náleží poskytovateli cena, na kterou má nárok podle smlouvy, ponížená o to, co poskytovatel ušetřil neprovedením Dodávky v plném rozsahu. V případě, že objednatel nebude mít zájem ponechat si rozpracované plnění, má poskytovatel nárok na náhradu účelně vynaložených nákladů na provedení Dodávky do doby doručení odstoupení od smlouvy.

XIII.
Doručování

1. Smluvní strany této smlouvy se dohodly následujícím způsobem na adrese pro doručování písemné korespondence, pokud není smlouvou stanoveno jinak:

a) adresa pro doručování objednateli je: Pardubický kraj Komenského nám. 125; 532 11 Pardubice, IDDS: z28bwu9.

b) adresa pro doručování poskytovateli je: [DOPLNÍ DODAVATEL], IDDS: [DOPLNÍ DODAVATEL].

2. Veškerá podání a jiná oznámení, která se doručují smluvním stranám, je třeba doručit datovou schránkou, osobně, nebo doporučenou listovní zásilkou s doručenkou, pokud není ve smlouvě stanoveno jinak.
3. Aniž by tím byly dotčeny další prostředky, kterými lze prokázat doručení, má se za to, že oznámení bylo řádně doručené třetím dnem po jeho odeslání v případě, že bylo odesláno prostřednictvím držitele poštovní licence.

XIV.
Závěrečná ustanovení

1. Smluvní strany prohlašují, že žádná část smlouvy nenaplňuje znaky obchodního tajemství ve smyslu § 504 občanského zákoníku.
2. Smluvní strany berou na vědomí, že nebude-li smlouva zveřejněna ani do tří měsíců od jejího uzavření, je následujícím dnem zrušena od počátku.
3. Smluvní strany této smlouvy se dohodly, že právní vztahy založené touto smlouvou se budou řídit právním řádem České republiky. Tato smlouva jakož i právní vztahy touto smlouvou neupravené se řídí občanským zákoníkem.
4. Případné spory vzniklé z této smlouvy budou řešeny dohodou smluvních stran a nebude-li dohody, pak podle platné právní úpravy věcně a místně příslušnými soudy České republiky.
5. V případě neplatnosti nebo neúčinnosti některého ustanovení této smlouvy nebudou dotčena ostatní ustanovení této smlouvy.
6. Smluvní strany se dohodly, že v případě zániku právního vztahu založeného touto smlouvou zůstávají v platnosti a účinnosti i nadále ustanovení, z jejichž povahy vyplývá, že mají zůstat nedotčena zánikem právního vztahu založeného touto smlouvou.
7. Právní jednání bylo schváleno dne [BUDE DOPLNĚNO] Radou Pardubického kraje usnesením [BUDE DOPLNĚNO].
8. Tuto smlouvu lze měnit, doplňovat a upřesňovat pouze oboustranně odsouhlasenými, písemnými a průběžně číslovanými dodatky, podepsanými oprávněnými zástupci obou smluvních stran.
9. Smlouva je vyhotovena ve třech stejnopisech, z nichž objednatel obdrží dva výtisky a poskytovatel jeden výtisk. Každý stejnopis této smlouvy má právní sílu originálu.

   Alternativně (před podpisem smlouvy se ponechá relevantní alternativa):

   Tato smlouva je v souladu § 211 odst. 3 zákona č. 134/2016 Sb. o zadávání veřejných zakázek ve znění pozdějších předpisů ve spojení se zákonem č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů, uzavřena elektronicky.
10. Obě smluvní strany potvrzují autentičnost této smlouvy a prohlašují, že si smlouvu včetně příloh přečetly, s jejím obsahem (včetně příloh) souhlasí, že smlouva byla sepsána na základě pravdivých údajů, z jejich pravé a svobodné vůle a nebyla uzavřena v tísni ani za jinak jednostranně nevýhodných podmínek, což stvrzují svým podpisem, resp. podpisem svého oprávněného zástupce.
11. Nedílnou součást této smlouvy tvoří:
    - Příloha č. 1: Specifikace díla (technická specifikace)
    - Příloha č. 2: Servisní služby

- Příloha č. 3: Nabídková cena – tabulka do ZD a nabídky
- Příloha č. 4: Seznam poddodavatelů
- Příloha č. 5: Seznam osob – členů realizačního týmu
- Příloha č. 6: Vzor akceptačního protokolu
- Příloha č. 7: Povinnosti poskytovatele vyplývající z finanční spoluúčasti evropských fondů na realizaci projektu

V Pardubicích dne ……

V …… dne ……

JUDr. Martin Netolický Ph.D.
hejtman Pardubického kraje

[DOPLNÍ DODAVATEL]

Příloha č. 1 smlouvy

Specifikace díla (technická specifikace)

Bude použita příloha č. 2 Zadávací dokumentace

Příloha č. 2 smlouvy

Servisní služby

Bude použita dodavatelem vyplněná příloha č. 3 Zadávací dokumentace

Příloha č. 3 smlouvy

Nabídková cena – tabulka do ZD a nabídky

Bude použita dodavatelem vyplněná příloha č. 4 Zadávací dokumentace

Příloha č. 4 smlouvy

Seznam poddodavatelů

Bude doplněno dodavatelem do následující tabulky

Název	IČ	Sídlo	Předmět plnění

Spolufinancováno Evropskou unií

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

Příloha č. 5 smlouvy

Seznam osob – členů realizačního týmu

Bude doplněno dodavatelem do následující tabulky

Jméno a příjmení	Role týmu	Telefon	Email

Spolufinancováno Evropskou unií

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

Příloha č. 6 smlouvy
Vzor akceptačního protokolu

AKCEPTAČNÍ PROTOKOL

Poskytovatel	[BUDE DOPLNĚNO]
Objednatel	**Pardubický kraj**
Smlouva	*Smlouva o dodávce HW a SW a o poskytování souvisejících služeb č.* [BUDE DOPLNĚNO]
Název Projektu	Kybernetická bezpečnost poskytovatelů ZS následné péče Pardubického kraje
Číslo Projektu	CZ.06.3.05/0.0/0.0/15_011/0006994
Datum předání	[BUDE DOPLNĚNO]
Předávací protokol č.	[BUDE DOPLNĚNO]

Popis dílčího plnění	Akceptováno bez výhrad	Akceptováno s výhradou	Neakceptováno

V Pardubicích dne …… V …… dne ……

Spolufinancováno Evropskou unií

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

[BUDE DOPLNĚNO]

[BUDE DOPLNĚNO]

Spolufinancováno Evropskou unií

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

Příloha č. 7 smlouvy

Povinnosti poskytovatele vyplývající z finanční spoluúčasti evropských fondů na realizaci projektu

Název projektu: Kybernetická bezpečnost poskytovatelů zdravotních služeb následné péče Pardubického kraje

Registrační číslo projektu: CZ.06.01.01/00/22_003/0000043

Název operačního programu: Integrovaný regionální operační program 2021-2027 (dále jen „IROP“)

Číslo a název výzvy: 3. výzva IROP - Kybernetická bezpečnost – SC 1.1 (MRR)

Řídící orgán: Ministerstvo pro místní rozvoj ČR

Manažerka projektu: Ing. Kristýna Boukalová, tel. 466 026 691, kristyna.boukalova@pardubickykraj.cz

1) Na každé faktuře bude jednoznačně uvedeno, že se jedná o projekt související s Integrovaným regionálním operačním programem (dále jen IROP) s názvem: **„**Kybernetická bezpečnost poskytovatelů zdravotních služeb následné péče Pardubického kraje**“,** registrační číslo projektu CZ.06.01.01/00/22_003/0000043. Rozdělení nákladů do výše uvedených projektů bude upřesněno při předání staveniště. Faktury musí obsahovat účel fakturovaných částek a budou přesně specifikovat jednotlivé položky - vše plně v souladu se zadávací dokumentací. Každá faktura musí mít přílohu, kde bude přiložen položkový rozpočet fakturovaných částek.
2) Poskytovatel si je vědom, že ve smyslu § 2, písm. e), zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů, je povinen poskytnout součinnost při výkonu finanční kontroly a to v případě, že k tomu bude objednatelem vyzván.
3) Poskytovatel se ve spolupráci s objednatelem zavazuje poskytnout kontrolním orgánům jakékoliv dokumenty vztahující se k realizaci projektu, podat informace a umožnit vstup do svého sídla a jakýchkoliv dalších prostor a na pozemky související s projektem nebo jeho realizací. Poskytovatel se zavazuje poskytnout na výzvu své daňové účetnictví nebo daňovou evidenci k nahlédnutí v rozsahu, který souvisí s projektem. Poskytovatel se dále zavazuje provést v požadovaném termínu, rozsahu a kvalitě opatření vedoucí k odstranění kontrolních zjištění a informovat o nich příslušný kontrolní orgán, objednatele a poskytovatele dotace.
4) Kontrolními orgány se rozumí osoby pověřené ke kontrole Evropskou komisí, Evropským účetním dvorem, Nejvyšším kontrolním úřadem, Ministerstvem financí ČR, Ministerstvem pro místní rozvoj ČR, Centrem pro regionální rozvoj ČR, popř. jiným poskytovatelem dotace či zprostředkujícím subjektem, jakož i dalšími orgány oprávněnými k výkonu kontroly (např. státní stavební dohled).
5) Poskytovatel bere na vědomí, že poskytovatel dotace je oprávněn provést u projektu nezávislý vnější audit. Poskytovatel je povinen při výkonu auditu spolupůsobit.
6) Poskytovatel je povinen spolupracovat s objednavatelem při zpracování monitorovacích zpráv (průběžných, etapových nebo závěrečných), žádostí o platbu, oznámení žadatele o změně projektu, závěrečného vyhodnocení akce.

7) Poskytovatel se zavazuje archivovat dokumenty související s dílem až do roku 2035.

8) Poskytovatel se zavazuje písemně poskytnout na žádost objednatele jakékoliv doplňující informace související s realizací projektu a to ve lhůtě stanovené objednatelem.

9) Další povinnosti poskytovatele vyplývají také z dokumentu „3. výzva IROP - Kybernetická bezpečnost – SC 1.1 (MRR)“ a dalších dokumentů dostupných na IROP - Ministerstvo pro místní rozvoj ČR - 3. výzva IROP - Kybernetická bezpečnost – SC 1.1 (MRR) (gov.cz). V případě rozporu v textu dokumentů s ustanoveními této smlouvy má přednost text smlouvy.

STAPRO s. r. o.

IČO 13583531

Pernštýnské náměstí 51, Pardubice-Staré Město, 530 02 Pardubice

(dále jen „Společnost“)

Věc: Závazek k součinnosti a garance poskytnutí rovných podmínek ve veřejné zakázce

Společnost je výhradním dodavatelem stávajících nemocničních informačních systémů (dále jen „Systém“) pro následující subjekty:

a) Léčebna dlouhodobě nemocných Rybitví
b) Odborný léčebný ústav Jevíčko
c) Albertinum, odborný léčebný ústav Žamberk
d) Nemocnice následné péče Moravská Třebová
e) Vysokomýtská nemocnice

V rámci plnění veřejné zakázky „Kybernetická bezpečnost poskytovatelů ZS následné péče Pardubického kraje“ (dále jen „VZ“) zadávané Pardubickým krajem, Komenského nám. 125, 532 11 Pardubice, IČO: 708 92 822 při realizaci projektu „Kybernetická bezpečnost poskytovatelů ZS následné péče Pardubického kraje“, registrační číslo CZ.06.01.01/00/22_003/0000043 bude nezbytné provést úpravy jednotlivých Systémů, případně poskytnout služby v návaznosti na uvedené Systémy tak, aby mohly být realizovány části předmětu VZ v oblastech navazujících na tento Systém.

Společnost se tímto zavazuje poskytnout veškerou součinnost nezbytnou k potřebným úpravám Systémů nebo poskytnutí služeb v návaznosti na uvedený Systém v rámci uvedené VZ všem dodavatelům, kteří o ní v rámci jejich zájmu o účast v zadávacím řízení na VZ požádají. Součinnost se Společnost zavazuje poskytnout všem dodavatelům za identických v místě a čase obvyklých podmínek, zejména cenových, dodacích a záručních.

Společnost specificky uvádí sazbu za člověkohodinu ve výši 1.700 Kč bez DPH, ostatní podmínky se budou odvíjet od rozsahu požadovaných činností a dodávaných částí Systémů, a to v případě totožných plnění za totožných cenových, dodacích a záručních podmínek.

Společnost si je vědoma, že zadavatel je v rámci zadávacího řízení povinen zajistit prostředí pro hospodářskou soutěž dodavatelů v rovných podmínkách bez toho, aby bylo vůči některým dodavatelům (uchazečům o tuto veřejnou zakázku) ze strany Společnosti, tedy unikátního dodavatele dílčího plnění, postupováno diskriminačním způsobem.

V Pardubicích dne (viz el. podpis)

……..

Ing. LEOŠ RAIBR

jednatel

STAPRO s. r. o.

LAURYN s.r.o.

IČ: 60113685

Sídlo: Pardubice - Staré Čívice, Přeloučská 255, PSČ 53006

(dále jen „Společnost“)

Věc: Závazek k součinnosti a garance poskytnutí rovných podmínek ve veřejné zakázce

Společnost je výhradním dodavatelem stávajících nemocničních informačních systémů (dále jen „Systém“) pro následující subjekty:

a) Rehabilitační ústav Brandýs nad Orlicí

V rámci plnění veřejné zakázky „Kybernetická bezpečnost poskytovatelů ZS následné péče Pardubického kraje“ (dále jen „VZ“) zadávané Pardubickým krajem, Komenského nám. 125, 532 11 Pardubice, IČO: 708 92 822 při realizaci projektu „Kybernetická bezpečnost poskytovatelů ZS následné péče Pardubického kraje“, registrační číslo CZ.06.01.01/00/22_003/0000043 bude nezbytné provést úpravy jednotlivých Systémů, případně poskytnout služby v návaznosti na uvedené Systémy tak, aby mohly být realizovány části předmětu VZ v oblastech navazujících na tento Systém.

Společnost se tímto zavazuje poskytnout veškerou součinnost nezbytnou k potřebným úpravám Systémů nebo poskytnutí služeb v návaznosti na uvedený Systém v rámci uvedené VZ všem dodavatelům, kteří o ní v rámci jejich zájmu o účast v zadávacím řízení na VZ požádají. Součinnost se Společnost zavazuje poskytnout všem dodavatelům za identických v místě a čase obvyklých podmínek, zejména cenových, dodacích a záručních.

Společnost specificky uvádí sazbu za člověkohodinu ve výši 1.600 Kč bez DPH, ostatní podmínky se budou odvíjet od rozsahu požadovaných činností a dodávaných částí Systémů, a to v případě totožných plnění za totožných cenových, dodacích a záručních podmínek.

Společnost si je vědoma, že zadavatel je v rámci zadávacího řízení povinen zajistit prostředí pro hospodářskou soutěž dodavatelů v rovných podmínkách bez toho, aby bylo vůči některým dodavatelům (uchazečům o tuto veřejnou zakázku) ze strany Společnosti, tedy unikátního dodavatele dílčího plnění, postupováno diskriminačním způsobem.

V Pardubicích dne (viz el. podpis)

……..	……..
Ing. Štěpán Lauryn	Ing. Radek Lauryn
Jednatel	jednatel
LAURYN s.r.o.	LAURYN s.r.o.

INTEGROVANÝ REGIONÁLNÍ OPERAČNÍ PROGRAM 2021–2027

OBECNÁ PRAVIDLA PRO ŽADATELE A PŘÍJEMCE

PŘÍLOHA 9

ČESTNÉ PROHLÁŠENÍ O OPATŘENÍCH K MEZINÁRODNÍM SANKCÍM

VERZE 3

Spolufinancováno Evropskou unií

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

ČESTNÉ PROHLÁŠENÍ

o opatřeních ve vztahu k mezinárodním sankcím přijatým Evropskou unií v souvislosti s ruskou agresí na území Ukrajiny vůči Rusku a Bělorusku

Číslo a název projektu: CZ.06.01.01/00/22_003/0000043, Kybernetická bezpečnost poskytovatelů zdravotních služeb následné péče Pardubického kraje

Název veřejné zakázky: „ Kybernetická bezpečnost poskytovatelů ZS následné péče Pardubického kraje“.

(dále jen „veřejná zakázka“)

DODAVATEL

Dodavatel (název, IČO)…….....

Zastoupen (jméno příjmení, funkce): .....

(dále jen „dodavatel“)

Prohlašuji, že jako dodavatel veřejné zakázky nejsem dodavatelem ve smyslu nařízení Rady EU č. 2022/576, tj. nejsem:

a) ruským státním příslušníkem, fyzickou či právnickou osobou, subjektem či orgánem se sídlem v Rusku,
b) právnickou osobou, subjektem nebo orgánem, který je z více než 50 % přímo či nepřímo vlastněný některým ze subjektů uvedených v písmeni a), nebo
c) fyzickou nebo právnickou osobou, subjektem nebo orgánem, který jedná jménem nebo na pokyn některého ze subjektů uvedených v písmeni a) nebo b).

Prohlašuji, že nevyužiji při plnění veřejné zakázky poddodavatele, který by naplnil výše uvedená písm. a) – c), pokud by plnil více než 10 % hodnoty zakázky.

Dále prohlašuji, že neobchoduji se sankcionovaným zbožím, které se nachází v Rusku nebo Bělorusku či z Ruska nebo Běloruska pochází a nenabízím takové zboží v rámci plnění veřejných zakázek.

Současně prohlašuji, že žádné finanční prostředky, které obdržím za plnění veřejné zakázky, přímo ani nepřímo nezpřístupním fyzickým nebo právnickým osobám, subjektům či orgánům s nimi spojeným uvedeným v sankčním seznamu v příloze nařízení Rady (EU) č. 269/2014 ve spojení s prováděcím nařízením Rady (EU) č.

2022/581, nařízení Rady (EU) č. 208/2014 a nařízení Rady (ES) č. 765/2006 nebo v jejich prospěch[1].

V případě změny výše uvedeného budu neprodleně zadavatele informovat.

Datum:
……

dodavatel

[1] aktuální seznam sankcionovaných osob je uveden na https://www.sanctionsmap.eu/