Příloha č. 3: Technická specifikace

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

OBSAH

Obsah 1

Využité zdroje 2

Seznam tabulek 2

Seznam zkratek a pojmů 3

1 Předmět plnění 6

2 Členění dokumentu 7

3 Rozsah dodávky a souvisejících služeb 8

3.1 Vymezení předmětu a rozsahu dodávky 8

3.1.1 Související služby a náležitosti dodávky 8

3.1.2 Dodávkou nedotčené oblasti stávajícího řešení 9

3.1.3 Vyloučení z dodávky 9

3.2 Východiska a připravenost 9

3.3 Základní požadavky na zabezpečení IS 10

3.4 Požadavky na dodávky 11

3.4.1 Obecné a společné požadavky 11

3.4.2 Zabezpečení systému elektronické pošty před škodlivým kódem 11

3.4.3 Komplexní ochrana koncové stanice, antivir, antimalware, firewall včetně centrální správy 16

3.4.4 Konfigurace systému elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů 18

3.4.5 Bezpečnostní požadavky 19

3.4.6 Implementační a provozní požadavky 20

3.5 Požadavky na služby 21

3.5.1 Realizace předmětu plnění 21

3.5.2 Seznámení s funkcionalitami, obsluhou dodávaných technologií 24

3.6 Záruky 24

4 Harmonogram 26

5 Místa plnění 27

6 Výchozí stav 28
6.1 Zdravotnická záchranná služba Královéhradeckého kraje (zadavatel) 28
6.2 Informační systémy k zabezpečení 28
6.2.1 IS ZOS 29
6.2.2 Elektronická pošta 35
6.3 Umístění IS ZOS, systému elektronické pošty a DC 36
6.4 Stav ostatních informačních a komunikačních technologií 36
6.4.1 Datové centrum, HW infrastruktura, systémový SW a technologie 36
6.4.2 Datové sítě 38
6.4.3 Síťová infrastruktura 38
6.4.4 Provoz 40
Konec dokumentu 40

Využité zdroje

Nejsou

Seznam tabulek

Tabulka 1: Seznam zkratek a pojmů 5
Tabulka 2: Předmět a rozsah dodávky 8
Tabulka 3: Východiska 10
Tabulka 4: Obecné a společné požadavky 11
Tabulka 5: Zabezpečení systému elektronické pošty před škodlivým kódem 16
Tabulka 6: Komplexní ochrana koncové stanice, antivir, antimalware, firewall včetně centrální správy 18
Tabulka 7: Konfigurace systému elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů 19
Tabulka 8: Bezpečnostní požadavky 20
Tabulka 9: Implementační a provozní požadavky 21
Tabulka 10: Dokumentace – požadavky na zpracování 23
Tabulka 11: Harmonogram 26
Tabulka 12: Místa plnění 27
Tabulka 13: Výčet IS k zabezpečení 29
Tabulka 14: IS ZOS 35
Tabulka 15: Umístění 36
Tabulka 16: Datové centrum, HW infrastruktura, systémový SW 38
Tabulka 17: Datové sítě 38

Tabulka 18: Síťová infrastruktura 39

SEZNAM ZKRATEK A POJMŮ

Zkratka/pojem	Význam
365x7x24	Poskytování služeb 365 dní v roce, 24 hodiny denně, 7 dnů v týdnu
ACL	Access Control List
AD	Microsoft Active Directory
API	Application Programming Interface – rozhraní pro programování aplikací
AVL	Systém sledování polohy vozidel
CD / CD-ROM / DVD / USB	Datový nosič
ČR	Česká republika
DB	Databáze
DC	Datové centrum
DMZ	Demilitarizovaná zóna
EKP	Elektronická karta pacienta
EU	Evropská unie
FW	Firewall
GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob
GIS	Geografický informační systém
GUI	Grafické uživatelské rozhraní
HW	Hardware
HTTPS	Hypertext Transfer Protocol Secure – v informatice protokol umožňující zabezpečenou komunikaci v počítačové síti
HZS (ČR)	Hasičský záchranný sbor České republiky
ICT	Informační a komunikační technologie
IOP	Integrovaný operační program
IP	Internet Protocol
IROP	Integrovaný regionální operační program

Zkratka/pojem	Význam
IS	Informační systém
IT	Informační technologie
IZS	Integrovaný záchranný systém
KII	Kritická informační infrastruktura
ks	Počet kusů
LAN	Lokální počítačová síť
LCT	Linkový radiový komunikační terminál radiové sítě Pegas/Matra
LDAP	Lightweight Directory Access Protocol – definovaný protokol pro ukládání a přístup k datům na adresářovém serveru
MS	Microsoft
MV ČR	Ministerstvo vnitra České republiky
MZD	Mobilní zadávání dat
NDIC	Národní dopravní informační centrum
NIS IZS	Národní informační systém IZS
OŘ	Operační řízení
OS	Operační systém
KHK	Královéhradecký kraj
PČR	Policie České republiky
PD	Projektová dokumentace
PNK	Prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018
PNP	Přednemocniční neodkladná péče
RADIUS	Remote Authentication Dial In User Service – Uživatelská vytáčená služba pro vzdálenou autentizaci
RCT	Radiový komunikační terminál radiové sítě Pegas/Matra
RUIAN	Registr územní identifikace, adres a nemovitostí
SaP	Síly a prostředky
SLA	Úroveň a podmínky poskytování služeb technické a technologické podpory
SMS	Krátká textová zpráva
SMTP	Simple Mail Transfer Protocol – internetový protokol určený pro přenos zpráv elektronické pošty (e-mailů) mezi přepravci elektronické pošty
SNMP	Simple Network Monitoring Protocol

Zkratka/pojem	Význam
SQL	Strukturovaný dotazovací jazyk pro práci v relačních databázích
SW	Software
TS	Technická specifikace
VPN	Virtuální privátní síť
VŘ	Výběrové řízení
VZ	Veřejná zakázka
WAF	Webový aplikační firewall
WAN	Rozsáhlá počítačová síť
ZD	Zadávací dokumentace
ZKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
ZOS	Zdravotnické operační středisko
ZVZ	Zákon o zadávání veřejných zakázek
ZZOS	Záložní zdravotnické operační středisko
ZZS	Zdravotnická záchranná služba (ve všeobecném významu)
ZZS KHK	Zdravotnická záchranná služba Královéhradeckého kraje

Tabulka 1: Seznam zkratek a pojmů

1 PŘEDMĚT PLNĚNÍ

Předmětem plnění veřejné zakázky (dílem) je komplexní dodávka a implementace technologií, dodávky SW pro realizaci technických bezpečnostních opatření dle § 5 odst. 3) zákona č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB) pro ochranu infomačních a komunikačních systémů Zadavatele, kterým je Zdravotnická záchranná služba Královéhradeckého kraje, před škodlivým kódem. Součástí plnění VZ jsou dále servisní služby na dobu neurčitou.

Zdravotnická záchranná služba Královéhradeckého kraje je základní složkou IZS a v souladu s legislativou plní úkoly i v případě mimořádných událostí a krizových situací, kdy mohou být těmito událostmi/situacemi zasaženy i informační systémy (IS) a komunikační systémy (KS) ZZS KHK a došlo by tedy k omezení, případně znemožnění plnění úkolů ZZS KHK.

Předmětem tedy je:

1. Zajištění interního systému elektronické pošty včetně jeho zabezpečení proti útokům ze sítě internet
2. Komplexní ochrana koncové stanice, antivir, antimalware, firewall včetně centrální správy
3. Konfigurace systému elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů

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 ZZS KHK s využitím těchto IS a KS.

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 a KS ZZS KHK vyplývajících z projevů kybernetických rizik (kybernetických bezpečnostních událostí).

Zvýšením bezpečnosti bude dosaženo nejen garantované provozování uvedených IS a KS, 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. 3 – 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 – Rozsah dodávky a souvisejících služeb –** 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 4 – Harmonogram** – kapitola obsahuje harmonogram realizace předmětu plnění VZ.
- **Kapitola 5 – Místa plnění** – kapitola obsahuje místa plnění v rámci realizace předmětu plnění VZ.
- **Kapitola 6 – 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 ROZSAH DODÁVKY A SOUVISEJÍCÍCH SLUŽEB

3.1 VYMEZENÍ PŘEDMĚTU A ROZSAHU DODÁVKY

Rozsah dodávky je následující:

#	Položka rozpočtu	Počet	Stručný popis položky	ID[1]
1	Zabezpečení systému elektronické pošty před škodlivým kódem	1 soubor	Dodávka technologií pro: 1. detekci spamů, nestandardní poštovní komunikace, definici politik pro antispam a filtrování komunikace. 2. ochranu proti webovým hrozbám Spyware/Adware/Phishing. 3. Možnost napojení na antivirové/antimalware programy. Součástí je dodávka, implementace, nastavení a napojení na systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí a související služby. Popis požadavků na předmět plnění je uveden v kap. 3.4.2.	H.10
2	Komplexní ochrana koncové stanice, antivir, antimalware, firewall včetně centrální správy	1 soubor	Dodávka systému komplexní ochrany koncových stanic (antivir, antimalware, firewall, včetně centrální správy). Součástí je dodávka, implementace, nastavení a napojení na systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí a související služby. Popis požadavků na předmět plnění je uveden v kap. 3.4.3.	H.10
3	Konfigurace systému elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů	1 soubor	Konfigurace systému elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů. Součástí je dodávka úprav nastavení, implementace, nastavení a napojení na systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí a související služby. Popis požadavků na předmět plnění je uveden v kap. 3.4.4.	H.5

Tabulka 2: Předmět a rozsah dodávky

3.1.1 Související služby a náležitosti dodávky

Součástí dodávky jsou dále následující služby a náležitosti:

1. Projektové řízení dodávky řešení

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

2. Zpracování návrhu dodávky a konfigurace technických opatření / technologií, související konzultace.
3. Dodávka, implementace, instalace, zapojení a konfigurace technických opatření / technologií.
4. Ověření funkčnosti dodaných technologií, zabezpečovaných IS a jejich (sou)částí.
5. Dodávka dokumentace dodaného vybavení a jeho částí (minimálně administrátorská dokumentace, dokumentace skutečného provedení/stavu po implementaci, systémová dokumentace). Dokumentace může být jedním dokumentem, nicméně musí obsahovat všechny relevantní informace.
6. Poskytnutí informací pro zpracování nebo aktualizaci bezpečnostní dokumentace s tím, že bezpečnostní dokumentace by měla plně reflektovat veškeré technologické a funkční změny.
7. Seznámení s obsluhou dodávaného systému a jeho budoucím provozem (správci).
8. Zařazení do provozního prostředí objednatele (dohled, zálohování apod.).
9. Provedení zkušebního provozu.
10. Poskytnutí záruky min. 5 roky na vybavení v rámci technických opatření.

Doplňující požadavky na implementaci:

1. Zajištění kontinuity provozu ZZS KHK. Po stránce nepřetržitého provozu ZZS KHK předpokládá pouze plánovanou odstávku 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.

3.1.2 Dodávkou nedotčené oblasti stávajícího řešení

Dodávkou nebudou dotčeny následující oblasti stávajícího řešení:

1. Současné systémy, technologie a pracoviště stávajícího zdravotnického operačního střediska (ZOS) zůstanou zachovány a nebudou negativně dotčeny realizací projektu.

3.1.3 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 (ZZS KHK) uvedený ve výchozím stavu a neuvedený v požadavcích.
3. Spotřební materiál využívaný v následném provozu informačních systémů neuvedený v rámci požadavků.

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

3.2 VÝCHODISKA A PŘIPRAVENOST

Pro řešení jsou stanovena následující východiska:

#	Popis východiska
1.	Zdravotnická záchranná služba Královéhradeckého kraje je základní složkou IZS a v souladu s legislativou plní úkoly i v případě mimořádných událostí a krizových situací, kdy může být těmito událostmi/situacemi zasaženo i zdravotnické operační středisko (ZOS) a došlo by tedy k omezení, případně znemožnění poskytování úkolů ZZS KHK.

#	Popis východiska
	Z uvedeného plyne, že informační a komunikační systémy podporující procesy poskytování PNP ze strany ZZS KHK musí být poskytovat své funkcionality i v případě mimořádných událostí a krizových situací, kdy může být těmito událostmi/situacemi zasaženo i zdravotnické operační středisko (ZOS).
2.	Současné řešení bylo realizováno v roce 2015 v projektu „Technologie pro Operační středisko ZZS Královéhradeckého kraje II“, který byl Královéhradeckým krajem realizován pro Zdravotnickou záchrannou službu Královéhradeckého kraje (ZZS KHK) v rámci Integrovaného operačního programu (IOP), výzvy č. 11. Současné řešení není možné nahradit, jen modernizovat při zachování veškeré stávající funkcionality a vybavení. Technologie a vybavení ZOS jsou předmětem zabezpečení technologiemi dodávanými v rámci dodávek uvedených dále v tomto dokumentu.
3.	Připravenost datových center bude zajištěna min. v následujícím rozsahu: 1. Dostatečně kapacitní napájení datového centra pro umístění technologií. 2. Klimatizace v datovém centru. 3. Strukturovaná kabeláž v rámci DC, mezi DC a mezi dodávanými technologiemi a zabezpečovanými IS. 4. Napojení na ostatní komunikační technologie.
4.	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.

Tabulka 3: Východiska

Další východiska jsou definována výchozím stavem uvedeným v kap. 6 – Výchozí stav.

3.3 Základní požadavky na zabezpečení IS

Základní požadavky na požadované řešení jsou následující:

1. Předmětem je zabezpečení následujících informačních systémů:
   a. Informační systém zdravotnického operačního střediska ZZS KHK – jedná se o primární IS sloužící pro hlavní činnost ZZS KHK, tj. poskytování PNP na území Královéhradeckého kraje.
   b. Elektronická pošta – jedná se o hlavní informační systém (IS) ZZS KHK zajišťující komunikaci mezi zaměstnanci ZZS KHK a podporu výkonu jejich činností.
2. Budou zajištěny všechny současné integrace uvedených IS a vazby na jiné IS a technologie nezbytné pro provoz ZZS KHK.
3. 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.
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.

3.4 POŽADAVKY NA DODÁVKY

V této kapitole jsou uvedeny požadavky na dodávky.

3.4.1 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 ZZS KHK.
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 (dále jen „PNK“), 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.
P.8	Soulad se Zákonem č. 239/2000 Sb. o integrovaném záchranném systému a o změně některých zákonů v aktuálním znění.
P.9	Soulad se Zákonem č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů v aktuálním znění.

Tabulka 4: Obecné a společné požadavky

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

3.4.2 Zabezpečení systému elektronické pošty před škodlivým kódem

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

Pro ochranu před škodlivým kódem požaduje dodávku řešení pro kontrolu provozu ze sítě internet pro elektronickou poštu i pro IS ZOS. Systém elektronické pošty je operačním řízením v IS ZOS využíván jako jeden z informačních kanálů, a proto je třeba zajistit maximální ochranu před škodlivým kódem a zajistit jeho trvalý chod.

Pro ochranu systému elektronické pošty se využívají tzv. Mail relay servery, které jsou dostupné ze sítě internet a provádění kontrolu veškeré přicházející (i odcházející) elektronické pošty a na interní poštovní servery již přenášejí zkontrolovanou komunikaci. Interní poštovní servery jsou tak z veřejné sítě nedostupné.

#	Požadavek
Bezpečná e-mailová brána	
P.10	Je požadováno plně redundantní řešení pro kontrolu poštovního provozu (EmailSecurity) s veřejnou sítí internet, včetně antispamové a antivirové ochrany. Řešení musí být formou virtuálního appliance do VMware.
P.11	Základní funkční požadavky: 1. Možnost nasazení v režimu MTA gateway nebo transparentní režim. 2. Možnost nasazení v režimu vysoké dostupnosti (včetně sdílení fronty) pro budoucí rozšíření. 3. Obousměrná a výrobcem podporovaná integrace s dalšími nabízenými bezpečnostními prvky (NG Firewall, sandbox) za účelem sdílení provozně telemetrických informací a informací o odhalených hrozbách (škodlivém kódu) sandboxovací technikou. 4. Ochrana proti škodlivému kódu, nevyžádané elektronické poště a uniku citlivých dat. 5. Podpora víceúrovňové detekce nevyžádané pošty (IP, domény, reputační databáze, ověření příjemce, DMARC, SPF, DKIM, proprietární funkce rozpoznávání nevyžádané pošty technikou výrobce, vyhledávání a kategorizace URI/URL, vyhledávání klíčových slov, behaviorální analýza). 6. Reakce na detekovaný spam minimálně: přidání tagu, přidání hlavičky, přeposlání e-mailu na jiný SMTP server, odmítnutí (reject), zahození (discard), uložení do karantény, přepsání adresy příjemce. 7. Možnost limitace v rámci SMTP navázané relace (počet zpráv od jednoho klienta za určitou dobu, maximální počet spojení od jednoho klienta za určitou dobu, podpora endpoint reputace, napojení na LDAP za účelem verifikace uživatelů; možnost omezení počtu HELO/EHLO v rámci jedné SMTP relace, možnost omezit počet e-mailových zpráv v rámci SMTP relace, možnost omezit počet příjemců v rámci adresátů e-mailu, možnost manipulace s hlavičkou mailu (odstranění Received hlavičky). 8. Antivirová kontrola (antimalware, funkce ochrany proti rychle se šířícím kampaním škodlivého kódu, heuristická funkce detekce škodlivého kódu, detekce dalších variant škodlivého kódu, odstranění aktivního obsahu PDF a kancelářských dokumentů, karanténa, odstranění škodlivých odkazů z emailů, AV kontrola musí být plně integrována s platformou Sandbox (viz níže), umožňující pokročilou ochranu před pokročilými typy hrozeb včetně tzv. zero-day útoků. Na rozdíl od firewallu tato integrace musí být v režimu pozdržení e-mailu ve frontě až do konce analýzy na sandboxu, sdílení signatur dynamicky vytvářených na platformě sandbox. 9. Podpora neutralizace dokumentů v příloze v dokumentech MS Office a PDF, při zachování původního typu dokumentu u dokumentů přijatých mimo organizaci. 10. Podpora tzv. „click protection“. 11. Podpora IPv6. 12. Podpora VLAN.

#	Požadavek
	13. Plnohodnotná integrace s LOG serverem a SIEM platformou. 14. Plnohodnotná integrace se síťovým dohledem (podpora SNMP (v2c, v3) včetně dostupnosti MIB souboru dodávaného výrobcem).
P.12	Minimální požadavky na EmailSecurity řešení: 1. Licenčně nezávislý model na počtu uživatelů, mailových schránek nebo IP adres (pokud jsou tyto funkce licencované, požadujeme dodání licence pro neomezený počet schránek). 2. Řešení musí být výkonově dimenzováno minimálně na 600 uživatelů a licencováno na 250 chráněných stanic (využíváno celkem 600 uživateli). 3. Propustnost min. 25 000 e-mailů za hodinu při průměrné velikosti e-mail cca 100 kB a prováděné kontrole na přítomnost škodlivého kódu a spamu. 4. Podpora ochrany minimálně 20 e-mailových domén. 5. Nabízené zařízení je možné provozovat v clusteru v režimu loadbalancing. 6. Využívání několika technologií pro detekci spamu – detekce dle slovníku, grafické filtry, PDF filter, URL posuzování, detekce spamu na základě reputace zdrojových IP adres. 7. Reputační filtrování na základě zdrojových IP adres odesílatele a reputační způsob blokování spamu na úrovni TCP spojení. 8. Možnost detekce detekci nestandardní poštovní komunikace (uchování podezřelých zpráv v karanténě do vyhodnocení výrobcem nebo zaslání nových definic). 9. Možnost nastavení anti-spam akce pro pozitivní nebo podezřelý spam: Doručit, zahodit, karanténa, doručit jako přílohu, přesměrovat. 10. Per-user anti-spam karanténa s ověřováním pomocí LDAP. 11. Definice whitelist a blacklist pro každého uživatele v karanténě. 12. Periodické zasílání notifikací o novém spamu v karanténě pro každého uživatele. 13. Možnosti uživatele pro práci se spamem v karanténě: Smazat, doručit, přidat do whitelistu. 14. Možnost označit/klasifikovat e-mail jako spam přímo z emailového klienta. 15. Detekce a klasifikace marketingových emailů, které nejsou spam. 16. Detekce viru uvnitř víceúrovňového archivu. 17. Možnost opravy zavirovaných příloh nebo jejich zahození 18. Automatická aktualizace všech antimalware signatur. 19. Per-user nebo per-group nastavení pro Anti-spam a Anti-virus akce pro příjemce či odesílatele. 20. Možnost vytváření sofistikovaných filtrů na e-mailovou komunikaci s možností filtrace na obsah hlaviček, těla i příloh e-mailu. 21. Kontrola příchozí i odchozí poštovní komunikace na jednom zařízení zároveň. 22. Filtrování obsahu a ochrana proti úniku dat: a. Podpora pro mezinárodní a multibyte umístění (nejlépe podpora UTF8). b. „Pattern matching“ uvnitř vícevrstvých archivů. c. Plná podpora regulárních výrazů pro „pattern matching“. d. Plnohodnotný filetype matching (ne na základě MIME type / filename). e. Detekce chráněných archivů. f. Možnost omezit maximální velikost přílohy nebo celého emailu.

#	Požadavek
	g. Filtrování na základě výsledku DKIM/SPF ověření. h. LDAP integrace pro filtrování obsahu. i. Per-user a per-group nastavení pro akce pro příjemce či odesílatele. j. Možnost nápravné akce: Karanténa, upozornění, zahodit email, zahodit přílohu, nahradit přílohu, přesměrovat. 23. Modifikace obsahu a zabezpečení dat: a. Per-user a per-group nastavení pro modifikaci obsahu a dat pro příjemce či odesílatele. b. Podmíněné přidání hlavičky do e-mailu, možnost přidat tzv. „footer“. c. Možnost odstranění hyperlinku URL z textu e-mailu. 24. Funkce SMTP – omezení protokolu např. na: a. Omezení maximálního počtu současných spojení per odesílatele. b. Omezení maximálního počtu zpráv per spojení. c. Omezení maximálního počtu příjemců v e-mailu. d. Omezení maximálního počtu příjemců za hodinu. 25. Administrace a management a. HTTPS Management console. b. Ověřování a autorizace administrátorů pomocí lokálních účtů a pomocí RADIUS. c. Napojení do centrálního dohledu pomocí SNMP. d. Podpora centrálního logování pomocí SYSLOG. e. Možnost definovat různé politiky (antispam a filtrovací politiky) pro jednotlivé uživatele nebo pro celé skupiny uživatelů. 26. Včetně možnosti integrace s MS AD a LDAP.
Sandbox	
P.13	Je požadováno řešení ochrany před zero-day škodlivým kódem, viry a malware (založeném na principu tzv. sandbox) ve formě HW appliance. Dodávané řešení musí být plně integrováno s dodávaným firewallem a řešením ochrany e-mailové komunikace. Plnou integrací se rozumí nativní integrace, umožňující obousměrnou komunikaci mezi firewallem a AS/AV řešením a platformou sandbox, tj. předávání souborů pro kontrolu, předávání detailních informací o kontrole zpět na firewall a AS/AV.
P.14	Požadovány jsou minimálně následující funkce: 1. Řešení musí poskytovat vícevrstvou ochranu před škodlivým kódem. Vícevrstvou ochranou je myšlena kombinace antivirové kontroly za pomoci signatur, emulace kódu a plnohodnotný sandbox (spuštění v reálném operačním systému). Všechny tyto úrovně musí být integrovány do jednoho zařízení a vzájemně spolupracovat. 2. Všechny prvky ochrany musí být poskytovány lokálně, nikoliv jako cloud služba. 3. Požadujeme řešení ve formě hardware appliance o velikosti maximálně 1RU. Řešení musí umožňovat paralelní běh až 6 operačních systémů. 4. Součástí dodávky musí být licence na min. 2 virtuálních systémů Windows. 5. Vše musí být součástí jedné hardware appliance. 6. Možnost integrace v režimu sniffer, on demand scan (předání souborů přes GUI), integrace se síťovým diskem, integrace s firewall a SMTP GW platformou (viz dále),

#	Požadavek
	integrace pomocí API (viz dále). Všechny metody musí být využitelné naráz a na jedné hardware appliance. 7. Plná a obousměrná integrace s platformou firewallu a SMTP brány. Obousměrnou komunikací se rozumí obousměrné předávání informací mezi platformou Sandboxu a firewallem, resp. SMTP bránou. 8. Řešení musí nabízet otevřené API jak pro možnost získaní informací o prováděných inspekcích a detekovaných hrozbách, tak pro možnost integrace s dalšími produkty. API proto musí umožňovat předat zařízení soubory k inspekci a následně získat informaci o výsledku včetně detailů o inspekci (detekované chování, screenshoty, videa, logy atd.…). Pokud tato funkce vyžaduje samostatnou licenci, tak tato musí být součástí dodávky. 9. Sandbox musí být nakonfigurován tak, aby nekomunikoval přímo do internetu. Z toho důvodu požadujeme jako součást řešení centrální management platformu, která bude nainstalovaná v samostatné DMZ s povoleným přístupem do internetu a se kterou bude Sandbox komunikovat. Výjimkou je komunikace virtuálních strojů do internetu, která bude vedena samostatným fyzickým portem a samostatným internetovým připojením. 10. U sandbox platformy nepožadujeme dodání vysoce dostupného řešení (HA), nicméně dodaná platforma musí tuto funkcionalitu podporovat s ohledem na možný další rozvoj sítě (včetně zvýšení výkonnosti formou active-active HA). To vše ale pouze za předpokladu, že zapojení do síťové infrastruktury, s ohledem na požadované funkce, nevyžaduje nasazení tzv v “inline režimu” a případný výpadek sandbox platformy neohrozí produkční komunikaci (komunikace uživatel do internetu, přístup uživatel do vnitřní sítě, e-mailová komunikace atd.). V opačném případě požadujeme dodání platformy sandbox ve vysoce dostupné HW konfiguraci, s požadovanou výkonností zajištěnou i při výpadku jednoho z uzlů sandbox clusteru. 11. Podporované operační systémy: Windows 7, Windows 8.1, Windows 10, Android, Linux, macOS. 12. Podpora zákaznické konfigurace Windows VM (zákazník si může připravit specifickou konfiguraci OS, využívanou jako standard v prostředí zákazníka). 13. Ochrana proti zjištění běhu v sandbox prostředí (anti evasion techniky). 14. Detekce komunikace s C&C centry. 15. Podpora detekce přístupu na kompromitované URL. 16. Funkce reportingu nalezených problémů (Součástí výsledné informace nesmí být pouze status čistý/škodlivý kód, ale kompletní informací včetně detailního popisu chování, packet capture, a v případě projevu malware v GUI také screenshoty). 17. Podpora kontroly minimálně následujících typů souborů: spustitelné soubory, JAVA, PDF, MS Office dokumenty, běžné multimediální formáty jako např. JPEG, QuickTime, MP3; archívy (ZIP/RAR/7ZIP/TNEF), asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm. 18. Podpora reportování ve standardních formátech (HTML, CSV, PDF, XML, …). 19. Oddělená konektivita pro systémovou/management komunikaci a pro komunikaci virtuálních strojů do internetu. 20. Automatická aktualizace signaturových databází.

#	Požadavek
	21. Automatická aktualizace VM zveřejněných výrobcem.
Společné požadavky	
P.15	Řešení e-mail security bude provozováno na infrastruktuře zajištěné Objednatelem v rámci součinnosti.
P.16	Součástí dodávky musí být instalace a konfigurace řešení včetně součinnosti při konfiguraci jednotlivých zařízení a aplikací a nastavení notifikací, a to včetně seznámení s funkcionalitami a obsluhou.
P.17	Je požadováno za 1 měsíc a za 3 měsíce vyhodnocení provozu a doladění pravidel/nastavení na základě získaných dat během provozu implementovaného systému a dle požadavků Zadavatele.
P.18	Napojení a předávání alertů a logů do systému analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí (konkrétní typ a přístup budou dodány v rámci součinnosti).
P.19	Je požadována dodávka nezbytných licencí, záruka na funkčnost, podpora aktualizace všech signatur a dodaného řešení po dobu 5 let.

Tabulka 5: Zabezpečení systému elektronické pošty před škodlivým kódem

3.4.3 Komplexní ochrana koncové stanice, antivir, antimalware, firewall včetně centrální správy

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

Prioritou je ochránit pracoviště přistupující do jednotlivých modulů operačního řízení před škodlivým kódem. Jedná se hlavně o tato pracoviště:

1. Dispečerská PC
2. Výjezdová PC (na výjezdových základnách)
3. PC a NB ostatních zaměstnanců využívajících OŘ
4. PC a NB ostatních zaměstnanců využívajících el. poštu

#	Požadavek
P.20	Je požadováno plně redundantní řešení pro komplexní ochranu koncových stanic (endpointy), antivir, antimalware, firewall včetně centrální správy (správa z jednoho místa).
P.21	Minimální požadavky na řešení: 1. Řešení musí být výkonově dimenzováno minimálně na 600 uživatelů a licencováno na 250 chráněných stanic/endpointů. 2. Ochrana pro OS Windows, MAC, Linux, Android, iOS a ChromeBook endpointy. 3. Řešení je možné provozovat v clusteru. 4. Centrální a jednotnou správu pokročilé antimalware ochrany pracovních stanic (centrální řízení, dohled a správa z jednoho místa). 5. Integrovaný firewall založený na analýze sítových aplikací na pracovních stanicích. 6. Možnost uzamknutí privilegovaných operací a úkonů před běžným uživatelem. 7. Automatická karanténa pracovní stanice v případě detekce bezpečnostní hrozby.

#	Požadavek
	8. Sběr a vyhodnocení telemetrických informací pracovních stanic. 9. Sběr informací o instalovaném SW na pracovních stanicích. 10. Politiky pro přístup k USB periferiím. Možnost zakázat nebo naopak povolit konkrétní USB zařízení na základě HW ID. 11. Možnost sledovat a shlédnout aktuální status aktivit na daném endpointu včetně bezpečnostních událostí. 12. Administrace a management: a. HTTPS Management console. b. Podpora centrálního logování pomocí SYSLOG. 13. Včetně možnosti integrace s MS AD a LDAP. 14. Implementace, aktualizace, nasazování: a. Centralizované nasazení a správa endpointů, včetně software updatů endpoint řešení spravovaných klientů. b. Možnost nasazení/instalace centrálního MSI balíčku na jednotlivé klienty pomocí GPO. 15. Možnost napojení na poštovní server pro zasílání varování a chyb systému. 16. Centrální správa endpointů, profilů, skupin apod. 17. Možnost dynamického seskupování endpointů dle významných informací (např. OS, certifikátu, instalovaného antivirového SW, souboru apod.). 18. Obousměrná a výrobcem podporovaná integrace s dalšími nabízenými bezpečnostními prvky, především Next Generation Firewall, za účelem sdílení provozně telemetrických informací a informací o odhalených hrozbách. 19. Integrace s dodávaným sandboxovacím systémem za účelem ochrany proti virům.
P.22	Požadavky na SW do koncových HW zařízení/endpointů: 1. Funkce automatického připojení do VPN před přihlášení uživatele do Windows. 2. Možnost autentikace klientů pomocí RADIUSu, LDAPu, TACACS+, certifikátem nebo ověřením oproti lokální databázi na endpoint manageru. 3. Podporované operační systémy: Windows 7, 8, 8.1, 10 (32 a 64 bit), Windows 11 (64 bit) Windows Server 2012 a výše, macOS 11+, 10.15, 10.14, iOS 9.0 a výše, Android 5.0 a výše, Linux Ubuntu 16.04 a výše, Red Hat 7.4 a výše a CentOS 7.4 a výše. 4. SSL VPN funkcionalita dostupná minimálně pro Windows, MAC, Android, IOS a Linux klienty. 5. IPsec VPN funkcionalita dostupná minimálně pro Windows, MAC a Android klienty. 6. Možnost aplikační firewallu pro Windows a MAC klienty. 7. Možnost web filteringu pro Windows, MAC, Android, IOS a Linux. 8. Antivirová ochrana s umělou inteligence pro Windows, MAC a Linux klienty. 9. Cloudový sandboxing pro Windows a MAC klienty. 10. Windows stanice musejí být chráněny ochranou proti ransomwaru. 11. Možnost správy konfiguračních profilů pomocí XML.
P.23	Centrální komponenty řešení budou provozováno na infrastruktuře zajištěné Objednatelem v rámci součinnosti.

#	Požadavek
P.24	Součástí dodávky musí být instalace a konfigurace řešení včetně součinnosti při konfiguraci jednotlivých zařízení a aplikací a nastavení notifikací, a to včetně seznámení s funkcionalitami a obsluhou.
P.25	Je požadováno za 1 měsíc a za 3 měsíce vyhodnocení provozu a doladění pravidel/nastavení na základě získaných dat během provozu implementovaného systému a dle požadavků Zadavatele.
P.26	Napojení a předávání alertů a logů do systému analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí (konkrétní typ a přístup budou dodány v rámci součinnosti).
P.27	Je požadována dodávka nezbytných licencí všech komponent (centrální i na endpointech), záruka na funkčnost, podpora aktualizace všech signatur a dodaného řešení po dobu 5 let.
P.28	Možnost dynamického rozšíření počtu spravovaných klientů prostým přikoupením licencí v počtu min. po 20 ks koncových endpointů včetně zapojení do centrální správy.
P.29	Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.

Tabulka 6: Komplexní ochrana koncové stanice, antivir, antimalware, firewall včetně centrální správy

3.4.4 Konfigurace systému elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů

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

#	Požadavek
P.30	Napojení na Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí a předávání následujících dat ze systému elektronické pošty: 1. Úspěšná a neúspěšná připojení k systému dostupnými protokoly 2. Využívání systému elektronické pošty jednotlivými uživateli 3. Dostupné bezpečnostní logy používaného systému 4. Dostupné chybové a provozní logy používaného systému Předávání veškerých logů systému do nástroje/rozhraní pro logování. Systém analýzy bezpečnostních logů a vyhodnocení kybernetických bezpečnostních událostí bude určen v rámci dodávky (součinnost objednatele).
P.31	Toto nastavení realizovat pro všechny komponenty systému elektronické pošty.
P.32	Předávání logů systému online prostřednictvím syslog služby.
P.33	Součinnost při konfiguraci FireWallu ZOS a konfigurace FireWallu ZZOS pro získávání informací o bezpečnostních událostech na prvcích FireWall, týkajících se systému elektronické pošty. Minimálně: 1. Odepření přístupu z dané IP adresy na systém (reputace dynamický ACL apod.) 2. IPS a AntiMalware události

#	Požadavek
	3. Identifikace chyb v protokolu
P.34	Systém dynamických ACL na základě parametrického vyhodnocení bezpečnostních logů systému. Dynamický ACL bude vytvářen prostřednictví analýzy logů na základě neoprávněného přístupu k systému. Pro vytváření dynamických ACL bude možné systémově nastavovat následující parametry: 1. Počet špatných přihlášení k danému protokolu 2. Minimální čas od posledního výskytu špatného přihlášení Publikace dynamického ACL pro systém elektronické pošty bude pro účely aktualizace pravidel FireWallu realizována web serverem jako standardní textový soubor s výčtem (list) IP adres (jedna IP na jednom řádku).
P.35	Nástroj/rozhraní pro logování bude zpracovávat i uvedený dynamický ACL pro systém elektronické pošty a zobrazovat časový průběh počtu IP adres obsažených v listu a upozorňovat na enormní nárůst.
P.36	Provedení konfigurace FireWallu ZOS pro implementaci dynamického ACL – aktualizace listu IP adres.
P.37	Stávající infrastruktura (HW) a systémový SW pro běh elektronické pošty po realizaci úprav zůstane beze změny, tj. nedojde ke změně konfigurace, parametrů, licencí systémového SW využívaných pro běh elektronické pošty.

Tabulka 7: Konfigurace systému elektronické pošty pro zaznamenávání činnosti (logů) do systému analýzy bezpečnostních logů

3.4.5 Bezpečnostní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.38	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.
P.39	Vybavení musí plnit podmínky zákona č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
P.40	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.41	Zabránění vstupu neautorizovaného subjektu do systému – zamezení možnosti přístupu neoprávněného subjektu.
P.42	Zajištění šifrované komunikace mezi všemi součástmi systému a pracovišti uživatelů, případně zajištění komunikace v odděleném síťovém prostředí.

#	Požadavek
P.43	Evidence přístupů všech uživatelů do systémů a technologií (logování) včetně časových údajů.
P.44	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.45	Veškeré logy budou dostupné pro externí systém pro sběr a vyhodnocení logů a kybernetických bezpečnostních událostí.

Tabulka 8: Bezpečnostní požadavky

3.4.6 Implementační a provozní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.46	Všechny komponenty musí být připraven na provoz 24x7x365 (non-stop).
P.47	Počet uživatelů informačních systémů se nezmění.
P.48	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.49	Instalace do prostředí objednatele uvedeného v kap. 6.4 – Stav ostatních informačních a komunikačních technologií a kap. 6.2 – Informační systémy k zabezpečení.
P.50	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.51	Dodávka OS na servery, včetně instalace do prostředí objednatele, vč. potřebných licencí, pokud se jedná o licencovaný OS.
P.52	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.53	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. Informace k zálohovacímu systému objednatele jsou uvedeny v kapitole 6.4.1 – Datové centrum, HW infrastruktura, systémový SW.
P.54	Zajištění administrátorských aplikací, konzolí pro všechny součástí systému (OS, DB, IS, …) pro zajištění konfiguračního managementu systému anebo jeho součástí.

#	Požadavek
P.55	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.56	Architektura řešení celého systému musí korespondovat s požadavky na jeho dostupnost, uvedenými v servisní smlouvě.
P.57	Synchronizace času všech zařízení s time serverem nebo zprostředkovaně přes centrální systém.

Tabulka 9: Implementační a provozní požadavky

3.5 POŽADAVKY NA SLUŽBY

3.5.1 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 4 – 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 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.

Název	Popis
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 10: 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.

3.5.2 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.

3.6 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.

4 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 účinnosti smlouvy na dodávku.
2	Analýza a návrh řešení	30	Zpracování analýzy a návrhu řešení pro potřeby upřesnění podmínek realizace.
3	Dodávka, implementace, instalace, konfigurace HW a SW infrastruktury a dodávaných technologií.	70	Dodávka a implementace HW, SW a síťové infrastruktury.
4	Ověření funkčnosti dodaných technologií.	80	Otestování funkčnosti technologií a ověření jejich plné funkčnosti.
5	Seznámení s funkcionalitami, obsluhou dodávaných technologií	80	Seznámení s funkcionalitami, obsluhou dodávaných technologií
6	Dodávka dokumentace dodaného systému a jeho částí.	80	Min. uživatelská dokumentace, dokumentace skutečného provedení, systémová dokumentace, projektová dokumentace.
7	Převedení do zkušebního provozu.	80	Převedení do zkušebního provozu, odstranění všech vad a nedodělků, dokončení realizace a převedení do ostrého provozu.
8	Ukončení realizace dodávky.	90	Součástí je zahájení doby provozu dodaného systému a poskytování servisních služeb.

Tabulka 11: 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.

5 MÍSTA PLNĚNÍ

Realizace předmětu plnění bude probíhat v následujících místech plnění:

Místo	Adresa	Předmět realizace
Sídlo a primární datové centrum	Hradecká 1690/2A, Hradec Králové PSČ: 500 12	Primární datové centrum ZZS KHK – dodávky v návaznosti na technologie umístěné v tomto DC a dodávka částí technologie. Primární lokalita IS elektronická pošta a záložní lokalita pro DC ZOS (zabezpečované IS a KS), DC je propojeno s DC ZOS. Sídlo ZZS KHK – místo předání výstupů projektu.
Datové centrum IS ZOS ZZS KHK	Pražská 230/153z, Hradec Králové PSČ: 500 04	Datové centrum IS ZOS ZZS KHK – dodávky v návaznosti na technologie umístěné v tomto DC a dodávka částí technologie. Primární lokalita, kde je provozován IS ZOS a kde je primární ZOS, DC je propojeno s primárním datovým centrem ZZS KHK. *Pozn.: lokalita označovaná také jako „Bláhovka“*

Tabulka 12: Místa plnění

6 VÝCHOZÍ STAV

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

6.1 ZDRAVOTNICKÁ ZÁCHRANNÁ SLUŽBA KRÁLOVÉHRADECKÉHO KRAJE (ZADAVATEL)

Kontext ZZS KHK v rámci řešení projektu je následující:

1. ZZS KHK plní úkoly zdravotnické záchranné služby k zajištění zvláštní zdravotní péče fyzickým osobám, které se náhle nebo nečekaně ocitly v ohrožení zdraví či života, tedy nepřetržitě zabezpečuje odbornou přednemocniční neodkladnou péči včetně přednemocniční péče o dárce a příjemce orgánů v souladu s příslušnými právními předpisy a pokyny zřizovatele a za plnění těchto úkolů odpovídá.
2. V rámci svých činností ZZS zajišťuje kvalifikovaný příjem, zpracování a vyhodnocení tísňových výzev k odborné zdravotnické první pomoci a určení nejvhodnějšího způsobu poskytování přednemocniční neodkladné péče.
3. ZZS je společně s PČR a HZS součástí a základní složkou Integrovaného záchranného systému (IZS), v rámci kterého vykonává svou činnost nejen v době míru, ale i v případě mimořádných událostí (dle zákona 239/2000 Sb.) a krizových situací (dle zákona 240/2000 Sb.) a další činnost dle legislativy.
4. ZZS KHK musí zajistit výkon veřejné správy v oblasti zdravotnické záchranné služby a podmínky pro zajištění připravenosti poskytovatele zdravotnické záchranné služby (ZZS KHK) na řešení i v případě mimořádných událostí a krizových situací (dle zákona č. 374/2011 Sb.) **a kybernetických bezpečnostních událostí** (dle zákona č. Zákon č. 181/2014 Sb.).
5. Pro tyto činnosti využívá informační systémy a technologie pro:
    a. podporu činností zdravotnického operačního střediska (ZOS) a posádek v terénu, včetně komunikace s posádkami, mezi posádkami a složkami IZS. Soubor technologií a subsystémů se nazývá informační systém zdravotnického operačního střediska (IS ZOS).
    b. Pro podporu komunikace mezi zaměstnanci ZZS KHK je využíván elektronická pošta.

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

6.2 INFORMAČNÍ SYSTÉMY K ZABEZPEČENÍ

V rámci projektu budou realizována opatření k zabezpečení ostatních informačních systémů (IS) a komunikačních systémů (KS) ZZS KHK. V rámci projektu nebudou realizována opatření k zabezpečení kritické informační infrastruktury (KII), žádného informačního systému základních služeb (ISZS) ani žádného významného informačního systému.

Zdravotnická záchranná služba Královéhradeckého kraje bude zabezpečovat své informační (IS). Stručný výčet IS je uveden v dalším textu této kapitoly.

Všechny uvedené IS a KS jsou umístěny, provozovány a využívány uživateli v sídle ZZS KHK nebo na adresách na území Královéhradeckého kraje uvedených v kap. 5.

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 ZZS KHK nebyla Národním úřadem pro kybernetickou a informační bezpečnost určena jako provozovatel základní služby podle §22a ZKB.

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

Název IS	Správce	Stručný popis	Typ
IS ZOS	Zdravotnická záchranná služba Královéhradeckého kraje	Informační systém a technologie pro podporu činností zdravotnického operačního střediska (ZOS) a posádek v terénu, vč. komunikace s posádkami, mezi posádkami a složkami IZS. Jedná se o soubor technologií a subsystémů společně zajišťující podporu uvedených procesů. Jedná se o primární IS sloužící pro hlavní činnost ZZS KHK, tj. poskytování PNP na území Královéhradeckého kraje.	Informační systém (IS)
Elektronická pošta	Zdravotnická záchranná služba Královéhradeckého kraje	Systém pro příjem a odesílání elektronické pošty v rámci komunikace ZZS KHK. Jedná se o hlavní informační systém (IS) ZZS KHK zajišťující komunikaci mezi zaměstnanci ZZS KHK a podporu výkonu jejich činností.	Infomační systém (IS)

Tabulka 13: Výčet IS k zabezpečení

Detaily k uvedeným IS jsou uvedeny v následujícím textu, a to jejich aktiva, části a další technické a provozní parametry relevantní pro dodávku.

6.2.1 IS ZOS

V této kapitole je detailně popsán IS ZOS, a to včetně dotčených aktiv.

6.2.1.1 Informační systémy a aplikační software ZOS

V této kapitole je uveden stávající stav informačních systémů a aplikačního software pro stávající ZOS:

IS, SW, subsystém	Stávající stav
IS OŘ	Jedná se o produkt SOS společnosti PER4MANCE s.r.o. využívaný ze strany 9 ZZS v ČR a min. jedné zahraniční ZZS (Maďarsko), tj. jedná se o široce používaný a standardizovaný produkt/systém. SOS je systém pro operační řízení dispečinku Zdravotnické záchranné služby (ZZS). Systém byl vyvinut na základě dlouhodobých zkušeností s provozem krajských ZZS se zahrnutím moderních požadavků na efektivní řízení Krajských záchranných operačních středisek (ZOS). Poskytuje funkcionalitu pro všechny činnosti ZOS ZZS počínaje náběrem tísňové výzvy (calltaking) přes operační řízení po vyhodnocení činnosti ZOS. Základní moduly implementované na ZZS KHK: 1. Dispečink

IS, SW, subsystém	Stávající stav
	2. Základna 3. Správa směn 4. Evidence směn 5. Svolávání 6. Statistiky 7. Kontrolní pracoviště 8. Administrace 9. Správa stanic Současně s tímto jsou realizovány následující integrace: 1. Interní (v rámci IS ZOS) a. Integrace telefonie – příjem tísňové výzvy. b. Integrace na GIS – zobrazení polohy tísňové výzvy, polohy výjezdu, lokalizace v mapě apod. c. Integrace na systém sledování vozidel – předávání výzvy k výjezdu, příjem a sledování stavů, sběr informací o výjezdu vozidel. d. EKP – předávání dat o pacientovi/pacientech k výjezdu pro posádku/posádky. e. Integrace na záznamový systém – připojování záznamů hovorů, přehrávání záznamů apod. f. Národní dopravně informační centrum – odesílání informací do NDIC o dopravních nehodách ze zaznamenaných událostí. g. Integrace telekomunikací a radiokomunikací – pro ovládání spojení a příjem statusů z RS. h. Integrace aplikace FirstResponder 2. Externí a. Národní informační systém IZS (NIS IZS) – výměna dat o událostech a SaP s tímto systémem. b. RUIAN – aktualizace dat adres dle Registru územní identifikace, adres a nemovitostí (data jsou čerpána z veřejného rozhraní RUIAN a je ukládána jejich offline kopie). c. Rozhraní pro příjem dat mobilní aplikace Záchranka d. Lokalizace volání info 35/ AML e. Rozhraní pro výzvy LZS + HS Součástí je řada dalších důležitých funckionalit, které jsou popsané v dokumentaci k IS. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.
GIS	Geografický systém je zajištěn produktem Fleetware od společnosti RADIUM s.r.o. Základní funkcionality jsou:

IS, SW, subsystém	Stávající stav
	1. Zobrazení mapových podkladů a základní práce s mapou na všech pracovištích dispečinku. 2. Zobrazování poloh a stavů vozidel ZZS ze systému sledování vozidel (AVL). 3. Zobrazování poloh událostí a SaP dalších složek IZS v rámci integrace na NIS IZS. 4. Lokalizace pro IS OŘ, vyhledávání v mapě a další geografické služby. Současně s tímto jsou realizovány následující integrace: 1. Interní (v rámci IS ZOS) a. IS OŘ – lokalizace, zobrazování výzev, událostí, poloh vozidel a další služby. b. Systém sledování vozidel (AVL) – čerpání poloh a stavů vozidel a jejich zobrazování v mapě. 2. Externí a. Národní informační systém IZS (NIS IZS) – výměna dat o událostech a SaP s tímto systémem. Součástí je řada dalších důležitých funckionalit, které jsou popsané v dokumentaci k IS. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.
EKP/MZD	Jedná se o produkt společnosti EMD dodaný a využívaný většinou ZZS v ČR. Elektronická karta pacienta (EKP) slouží pro zaznamenávání všech relevantních údajů o výjezdech a pacientech v rámci těchto výjezdů. Data jsou na vstupu čerpána z IS OŘ a následně během nebo po ukončení výjezdu z MZD, kontrolována a následně zpracována do formy pro vykazování pojišťovnám. Mobilní sběr dat (MZD) o pacientech slouží pro zadávání dat o pacientech v rámci výjezdu ZZS v terénu prostřednictvím mobilních zařízení (tabletů) a následně jejich předávání do centrálního systému EKP pro následné zpracování. Systémy poskytují následující funkce: 1. Přebírání dat o výjezdu z IS OŘ (součástí integrace). 2. Posílání dat do mobilních zařízení posádek v terénu. 3. Funkčnost pro vyplnění posádkami v terénu. 4. Elektronické podepisování certifikátem uživatele a biometrickým podpisem přebírajícího zdravotníka cílového zdravotnického zařízení. 5. Předávání Zprávy o výjezdu elektronickou cestou do Archivů zdravotnické dokumentace projektu eHealth. 6. Předání z MZD zpět do EKP. 7. Přebírání dat ze systému sledování vozidel. 8. Následné úpravy, dopracování, kontrola dat na výjezdových základnách. 9. Předávání do IS Pojišťovna. Současně s tímto jsou realizovány následující integrace:

IS, SW, subsystém	Stávající stav
	1. Interní (v rámci IS ZOS) a. IS OŘ – přebírání dat k výjezdu pro následné předání posádkám. b. Nahrávací systém (ReDAT) – přebírání lokalizace volajícího. c. Systém sledování vozidel (AVL) – informace o výjezdu z vozidel. d. IS Pojišťovna – předávání zpracovaných dat z výjezdu pro vyúčtování zdravotním pojišťovnám. 2. Externí a. eHealth systém KHK – výměna a elektronická archivace zdravotnické dokumentace na území KHK. Součástí je řada dalších důležitých funckionalit, které jsou popsané v dokumentaci k IS. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.
IS Pojišťovna	Jedná se o produkt společnosti EMD dodaný a využívaný většinou ZZS v ČR. Slouží pro vyúčtování poskytnuté zdravotnické péče zdravotním pojišťovnám. Současně s tímto jsou realizovány následující integrace: 1. Interní (v rámci IS ZOS) a. EKP/MZD – přebírání dat o pacientech a výjezdech pro vyúčtování. 2. Externí a. Informační systémy zdravotních pojišťoven. Součástí je řada dalších důležitých funckionalit, které jsou popsané v dokumentaci k IS. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.
Systém sledování vozidel (AVL)	Jedná se o produkt Fleetware od společnosti RADIUM s.r.o. Základní funkcionality jsou: 1. Sledování polohy a stavu vozidel ZZS. 2. Předávání těchto stavů, vč. doprovodných údajů z vozidel do IS OŘ a EKP. 3. Předávání dat pro zobrazení polohy a stavů vozidel v mapě. 4. Zasílání výzvy do vozidel. 5. Předávání dat do elektronické knihy jízd (EKJ). Současně s tímto jsou realizovány následující integrace: 1. Interní (v rámci IS ZOS) a. IS OŘ – poskytování stavů vozidel a výjezdů. b. GIS – zobrazování poloh a stavů vozidel v mapě. c. Poskytování poloh a stavů vozidel do NIS IZS v rámci součinnosti. d. EKJ – elektronická kniha jízd. 2. Externí

IS, SW, subsystém	Stávající stav
	a. Národní informační systém IZS (NIS IZS) – výměna dat o událostech a SaP s tímto systémem. Součástí je řada dalších důležitých funckionalit, které jsou popsané v dokumentaci k IS. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.
Elektronická kniha jízd (EKJ)	Elektronická kniha jízd přebírá data ze systému AVL a umožňuje vedení a sledování provozu vozidel. Stávající Elektronická kniha jízd (EKJ) je produkt Fleetware jehož výrobcem je společnost RADIUM s.r.o. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.
Svolávací systém	Je součástí IS OŘ – viz výše. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.
Telefonní ústředna	Telefonní ústředna je produkt Cisco Call Manager. Telefonní ústředna připojená na příjem tísňové linky 155 u telekomunikačního operátora. Telefonní ústředna je interně napojena na: 1. Nahrávací systém (ReDAT) pro nahrávání veškerých hovorů a přebírání lokalizace hovorů. 2. Integrace telefonie a radiofonie pro řízení a obsluhu volání přes ústřednu. Součástí je řada dalších důležitých funckionalit, které jsou popsané v dokumentaci k IS. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.
Záznamový systém (ReDAT)	Jedná se o produkt ReDAT společnosti RETIA, a.s. Záznamový systém (ReDAT) slouží pro záznam telefonních hovorů na tísňové lince, záznam všech hovorů na ZOS, a to jak telefonních, tak radiofonních. Nadstavbovou částí je subsystém eXperience pro přehrávání a analýzu zvukových záznamů.

IS, SW, subsystém	Stávající stav
	Záznamový systém je integrována na: 1. Telefonní ústřednu – záznam hovorů. 2. Integraci telefonie a radiofonie – pro záznam radiového hovoru. 3. IS telekomunikačního operátora – přebírání polohy volajícího v rámci příjmu tísňové výzvy. 4. IS OŘ – předávání polohy volajícího v rámci příjmu tísňové výzvy. Součástí je řada dalších důležitých funckionalit, které jsou popsané v dokumentaci k IS. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.
Integrace telefonie a radiofonie	Jedná se o produkty společnosti TTC MARCONI s.r.o. Integrace telefonie a radiofonie zajišťuje propojení IS OŘ s telefonií (telefonní ústředna), obsluhou radiové sítě Pegas/Matra MV ČR, záznamovým zařízením a poskytuje obsluze jednotný, a hlavně jednoduchý systém obsluhy pomocí dotykové obrazovky na pracovišti operátora. Základní funkcionality a integrace jsou: 1. Zajištění integrace a obsluhy telefonní komunikace prostřednictvím telefonní ústředny. 2. Zajištění integrace a obsluhy radiofonní komunikace prostřednictvím radiové sítě Pegas/Matra. 3. Zajištění integrace a obsluhy radiofonní komunikace prostřednictvím analogové radiové sítě ZZS. 4. Integrace s IS ZOS – volání, návaznost hovorů na výzvy a události. 5. Záznamové zařízení (ReDAT) – nahrávání radiofonní komunikace. 6. Poskytnuté aplikace na dotykové obrazovce obsluhy. Součástí je řada dalších důležitých funckionalit, které jsou popsané v dokumentaci k IS. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.
Integrace se systémem Pegas (CC-API)	CC-API slouží jako integrační rozhraní pro napojení informačních systémů a aplikačního SW k radiové síti PEGAS/TETRA a TETRAPOL. CC-API je produktem společnosti AIRBUS a výhradním dodavatelem technologie PEGAS/TETRA a TETRAPOL je společnost Pramacom Prague spol. s r.o. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu. Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.

Tabulka 14: IS ZOS

6.2.1.2 Pracoviště ZOS

Celkový počet pracovišť: 6 ks + 1 ks pro vedoucího směny + 1 ks testovací pracoviště, následující vybavení platí pro každé pracoviště jednotlivě.

Pracoviště ZOS jsou vybavena následovně:

1. Pracovní stanice PC Dell Optiplex 3050 (3x výstup na LCD).
2. 3x LCD monitory 24“, full HD (1920x1080), audiolišta.
3. 1x dotykový LCD / touchscreen 19“ pro ovládání integrace telefonie a radiofonie.
4. Klávesnice (USB).
5. Drátová myš (USB).
6. Bezdrátová Bluetooth náhlavní souprava připojená k integraci telefonie a radiofonie.
7. OS Windows 10, 64 bit.

6.2.2 Elektronická pošta

Systém pro příjem a odesílání elektronické pošty v rámci komunikace ZZS KHK. Část primární činnosti ZZS KHK, tj. poskytování PNP není podpořena IS ZOS (popsaný v předchozí kapitole), protože se jedná o ad-hoc postupy při situacích, které nejsou zcela běžné a vyžadují individuální přístup. Jedná se o nestandardní situace v běžném provozu, mimořádné události, krizové situace a samozřejmě kybernetické bezpečnostní události, případně incidenty. Současně s tímto není do primárních procesů v IS ZOS zapojeno vedení a technickohospodářský personál ZZS KHK zajišťující podporu hlavní činnosti ZZS KHK, tj. poskytování PNP.

Bez zajištění výměny informací (dokumentů, dat) mezi uvedenými skupinami uživatelů a při uvedených situacích, není možné garantovat poskytování PNP ze strany ZZS KHK, protože nebude možné řešit provozně technické problémy provozu při poskytování PNP.

Pro zajištění komunikace a výměny informací (dokumentů, dat) za uvedených situací a mezi uživateli zajišťující řízení poskytování PNP (personál ZOS) a vedením, resp. technickohospodářskými pracovníky, je využíván informační systém elektronické pošty.

Jedná se o hlavní informační systém (IS) ZZS KHK zajišťující komunikaci mezi zaměstnanci ZZS KHK a podporu výkonu jejich činností jak při standardních situacích, tak při nestandardních situacích, jak je uvedeno dříve v tomto textu.

Elektronická pošta je provozována jako samostatný informační systém ZZS KHK a je provozována v datovém centru ZZS KHK, tj. nejedná se o hosting ani službu.

Všichni uživatelé v rámci personálu ZZS KHK mají instalovány klienty tohoto IS, případně jsou napojení z obdobných klientů v rámci mobilních a desktopových zařízení.

Přístup je na základě identifikace a autorizace uživatele (v současné době bez napojení na AD), nicméně neprobíhá systematický sběr logů (provozních dat) a vyhodnocení kybernetických bezpečnostních událostí.

Elektronická pošta je provozována následujícím způsobem:

1. Je provozována v primárním datovém centru ZZS KHK – detaily viz kap. 6.3 – Umístění
2. Systém elektronické pošty využívá systém Kerio Connect ve verzi 9.x na OS Debian
3. Aktiva jsou sdílenými aktivy v rámci primárního DC v rámci samostatného virtuálního serveru. V rámci projektu budou zabezpečena jen centrální aktiva v DC
4. Provoz je zajištěn v režimu 7x24x365 – Elektronická pošta sice není kritickým systémem, ale je provozována nonstop z důvodu specifického provozu ZZS

5. Součástí projektu je zajištění Nástroje pro ochranu před škodlivým kódem, tj. technické opatření „e) nástroj pro ochranu před škodlivým kódem“
6. Součástí projektu jsou nástroje pro sběr dat a vyhodnocení kybernetických bezpečnostních událostí, tj. technické opatření „h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí“. Nástroje pro sběr dat a vyhodnocení kybernetických bezpečnostních událostí budou také zpracovávat i bezpečnostní logy centrálního mailového systému ZZS a vyhodnocovat tak případné bezpečnostní události v rámci systému elektronické pošty.

6.3 Umístění IS ZOS, systému elektronické pošty a DC

V následující tabulce jsou uvedena umístění IS ZOS:

Místo	Adresa	IS	Předmět realizace
Sídlo a primární datové centrum	Hradecká 1690/2A, Hradec Králové PSČ: 500 12	Elektronická pošta (primární DC) IS ZOS (záložní servery)	Sídlo ZZS KHK a primární část administrativního provozu a využívání elektronické pošty (zabezpečovaný IS).
Zdravotnické operační středisko ZZS KHK (DC, dispečink)	Pražská 230/153z, Hradec Králové PSČ: 500 04	IS ZOS (DC IS ZOS) Elektronická pošta (uživatelé)	Datové centrum IS ZOS ZZS KHK, všechna aktiva IS ZOS umístěná v tomto DC. Dispečerská pracoviště ZOS, kde jsou aktiva (pracoviště) operátorů ZOS. *Také označováno jako „Bláhovka“.*
Záložní datové centrum ZZS KHK	Areál LZS Fakultní nemocnice Sokolská 581 Hradec Králové PSČ: 500 12	Záložní DC ZZS KHK	Záložní/zálohovací datové centrum ZZS KHK – umístění zálohovacích a souvisejících technologií, zálohování systémů a technologií do této lokality.

Tabulka 15: Umístění

6.4 Stav ostatních informačních a komunikačních technologií

V této kapitole je uveden základní popis výchozího stavu jednotlivých prvků ostatních informačních a komunikačních technologií.

6.4.1 Datové centrum, HW infrastruktura, systémový SW a technologie

V následující tabulce je uveden popis datového centra, HW infrastruktury a systémového SW:

Parametr	Údaj(e), parametry a informace
Datové centrum IS ZOS (Lokalita Bláhovka)	
Záložní zdroj el. energie	Záložní napájení je využíváno v rámci napájení serverovny HZS, zajištěné jak UPS, tak motorgenerátorem.

Parametr	Údaj(e), parametry a informace
HW infrastruktura	
Rackové skříně	Veškerá technologie v rámci serverovny je umístěna v několika RACK skříních.
Servery	Jako virtualizační servery je využíváno celkem pět serverů DELL PowerEdge. Pro další potřeby jsou provozováno ještě další tři samostatné servery DELL PowerEdge a jeden HP ProLiant. Servery jsou osazeny síťovým rozhraním jak na technologii Gigabit ethernet, tak také TenGigabitethernet.
Disková úložiště	Úložiště je realizováno diskovým polem DELL SCv3020 10Gbps iSCSI a doplněno polem pro odkládání záloh QNAP NAS, který je také osazený 10Gbit rozhraním. Pro komunikaci diskových polí jsou vyhrazeny 10Gbps switche DELL, které tak tvoří infrastrukturu pro iSCSI.
Zálohování	Zálohování virtualizovaného prostředí je realizováno v rámci nastavených zálohovacích scénářů pomocí SW Veeam Backup pro VMware, případně prostou kopií dat na záložní NAS.
Systémový SW	
Operační systémy	V rámci dodávky virtualizačních serverů byly dodány licence Windows Server 2012 Datacenter. Pro některé servery je využit OS Linux v různých distribucích.
Virtualizační SW	Pro virtualizační servery je využito licence VMware Essentials Plus kit, který je určen pro 3 dvouprocesorové servery. Pro další dva servery je využito Oracle virtualizace.
DB	Pro provoz jsou využity databázové licence, a to jak ORACLE, tak Microsoft SQL server.
Dohled	Je realizován jako služba v rámci maintenance smlouvy s dodavatelem a za pomoci jeho prostředků.
Primární (centrální) datové centrum (Lokalita Hradecká)	
Záložní zdroj el. energie	Záložní napájení je zajištěno jak UPS, tak motorgenerátorem.
HW infrastruktura	
Rackové skříně	Veškerá technologie v rámci serverovny je umístěna v RACK skříni.
Servery	Jako virtualizační servery jsou využívány 2 servery DELL PowerEdge. Pro další potřeby je provozován ještě jeden samostatný servery DELL PowerEdge pro zálohu klíčového SW IS ZOS. Servery jsou osazeny síťovým rozhraním jak na technologii Gigabit ethernet, tak také TenGigabitethernet.
Disková úložiště	Úložiště je realizováno diskovým polem DELL SCv3020 10Gbps iSCSI a doplněno polem pro odkládání záloh QNAP NAS, který je také osazený 10Gbit rozhraním. Pro komunikaci diskových polí jsou využity přímo core switche HP datového centra (10Gbit) a fyzická rozhraní SAS serverů a diskového pole.

Parametr	Údaj(e), parametry a informace
Zálohování	Zálohování virtualizovaného prostředí je realizováno v rámci nastavených zálohovacích scénářů pomocí SW Veeam Backup pro VMware.
Systémový SW	
Operační systémy	V rámci dodávky virtualizačních serverů byly dodány licence Windows Server 2016 Datacenter. Pro některé servery je využit OS Linux v různých distribucích.
Virtualizační SW	Pro virtualizační servery je využito licence VMware Essentials Plus kit, který je určen pro 3 dvouprocesorové servery.
DB	Pro záložní server je využita databázová licence ORACLE.
Dohled	V rámci infrastruktury je využíván produkt HP IMC pro dohled a monitoring.
Záložní/zálohovací datové centrum (Lokalita LZS)	
Záložní zdroj el. energie	Záložní napájení je zajištěno jen UPS.
HW infrastruktura	
Rackové skříně	Veškerá technologie v rámci serverovny je umístěna v RACK skříni.
Dohled	V rámci infrastruktury je využíván produkt HP IMC pro dohled a monitoring (společný s primárním DC).

Tabulka 16: Datové centrum, HW infrastruktura, systémový SW

6.4.2 Datové sítě

V rámci projektu budou využity následující sítě:

Datová síť	Popis
WAN ZZS	Bude využita pro komunikaci mezi lokalitami z důvodu nutné výměny dat souvisejících s realizací a provozem projektu.
NIS IZS / PČR	Napojení na služby NIS IZS a LCT terminály Pegas/Matra. Síťový provoz tohoto napojení bude v rámci dodaných výstupů projektu monitorován.
Internet	V centrální lokalitě je zajištěno připojení k internetu, které bude možné využít i pro požadavky technologií v rámci realizace a provozu projektu.

Tabulka 17: Datové sítě

6.4.3 Síťová infrastruktura

V následující tabulce je uveden popis síťové infrastruktury:

Parametr	Údaj(e), parametry a informace
Primární datové centrum ZZS	
Směrovače	Lokality ZZS jsou propojeny do jedné WAN sítě prostřednictvím VPN WAN. Pro tyto účely jsou všechny lokality vybaveny routery Cisco, na kterých jsou nakonfigurovány

Parametr	Údaj(e), parametry a informace
	IPSec tunely do obou centrálních lokalit. Správa těchto routerů jsou zajištěna servisní maintenance smlouvou s dodavatelem.
Firewally	V rámci centrálních lokalit jsou umístěny centrální FireWally FortiGate, které zajišťují zabezpečení WAN ZZS do sítě internet a v rámci konfigurace centrálního FW jsou ukončovány i VPN přístupy pracovníků ZZS a externích firem do sítě ZZS. FireWall odděluje interní síť ZZS nejenom od sítě internet, ale i od ostatních externích sítí jako je NIS IZS a AKČR apod.
LAN	Lokalita Bláhovka: V rámci DC IS ZOS jsou využity LAN prvky na bázi switchů. Přičemž centrální stack switchů Cisco 3850 realizuje i routrování VLAN segmentů LAN sítě. Lokalita Hradecká: V rámci Primárního DC jsou využity LAN prvky na bázi switchů. Přičemž centrální stack switchů HP 5800 realizuje i routrování VLAN segmentů LAN sítě.
Připojení pracovišť ZOS	Vlastní připojení pracovišť ZOS je realizováno tak, aby výpadek jednoho prvku neznamenal výpadek celého ZOS, ale maximálně poloviny pracovišť.
Připojení k lince 155	Telefonní ústředna operačního řízení Cisco Call Manager je napojena prostřednictvím hlasové brány a rozhraním ISDN30 do veřejné telefonní sítě. ISDN30 je vyhrazena pro používání linky 155 a pro potřeby dispečinku (operačního řízení). Telefonní ústředna operačního řízení je propojena k SIP trunk a k objektové ústředně.
Připojení k síti NIS IZS – MV ČR (PČR)	V rámci serverovny dispečinku (DC IS ZOS) je realizováno i napojení na síť NIS IZS a síť PČR. Toto je realizováno samostatnými zálohovanými linkami ve správě NAKIT a tuto síť garantuje MV ČR.
Připojení ke krajské síti	ZZS má v lokalitě dispečinku realizováno i napojení na krajské nemocnice v rámci IS eHealth a síť AKČR.
Připojení k internetu	V obou centrálních lokalitách je i centrální napojení do sítě internet. Toto připojení je zabezpečeno FireWallem (viz výše). Poskytovatelem připojení do sítě internet je CESNET. Záložní připojení je zajištěno nezávislým lokálním operátorem HK Free.
Datové centrum PČR	
Aktivní prvky	Připojení do datového centra PČR je realizováno samostatným L2 datovým okruhem určeným pouze pro připojení k LCT terminálů. Na straně PČR je umístěn switch, do kterého je připojena veškerá technologie na straně PČR. Na straně ZZS je vyvedeno do centrálního switche Cisco 3850.
Radiové terminály Pegas/Matra (LCT)	V lokalitě PČR je umístěno celkem 7 LCT terminálů propojených do sítě Pegas/Matra.

Tabulka 18: Síťová infrastruktura

6.4.4 Provoz

Provoz stávajícího řešení je zajišťován s následujícími parametry:

1. Provoz systému je v režimu 7x24x365 – jedná se o kritický systém, jehož služby jsou uživatelům k dispozici nonstop, protože ZZS poskytuje služby a plní své úkoly nonstop.
2. IS ZOS je provozován jako vysoce dostupný systém s řadou redundantních prvků přispívajících k vysoké dostupnosti a zajištění funkčnosti i v případech výpadků některých prvků.
3. V rámci provozu je zajištěn dohled, jak je uvedeno dříve v tomto dokumentu
4. V rámci provozu je zajištěno zálohování, jak je uvedeno dříve v tomto dokumentu
5. Technická a technologická podpora systému:
    a. Je zajišťována v režimu 7x24x365, aby byla zajištěna vysoká dostupnost dle předchozího bodu
    b. Součástí je maintenance technologií a dodaného SW, technická a technologická podpora nad rámec záruky s kratšími SLA než v případě záruky
    c. Je poskytován 1st level support, vyhodnocení hlášených problémů a řešení závad ze strany dodavatele a poskytovatele služeb technické a technologické podpory
6. Administrace systému je v zodpovědnosti správců ZZS KHK.
7. V rámci provozu také probíhají:
    a. Nezbytné úpravy systému vyplývající ze změn legislativy, vyhlášek, případně dalších závazných dokumentů
    b. Rozvoj systému v návaznosti na nové potřeby ZZS KHK
    c. Pozáruční servis HW a SW infrastruktury

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

KONEC DOKUMENTU