Příloha č. 1: Technická specifikace

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

Obsah

Využité zdroje

Nejsou

Seznam tabulek

SEZNAM ZKRATEK A POJMŮ

Zkratka/pojem	Význam
ČR	Česká republika
DC	Datové centrum
EU	Evropská unie
GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob
ICT	Informační a komunikační technologie
IROP	Integrovaný regionální operační program
IS	Informační systém
KB	Kybernetická bezpečnost
KHK	Královéhradecký kraj
LZS	Letecká záchranná služba
SW	Software
VoKB	Vyhláška o kybernetické bezpečnosti
ZoKB	Zákon o kybernetické bezpečnosti
ZOS	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:

1. Bezpečnostní audit – provedení bezpečnostního auditu, jehož součástí bude provedení analýzy rizik ve vztahu k zabezpečovaným IS a technologiím, a který bude sloužit jako jeden z podkladů pro zavedení systému řízení bezpečnosti informací o opatření k zjištěným neshodám a o relevantní doporučení vyplývající z bezpečnostního auditu.
2. Bezpečnostní politika a dokumentace – vytvoření bezpečnostní dokumentace pro práci v kyberprostoru zadavatele v souladu s legislativou a best-practices.

Veškeré výstupy musí být zpracovány v souladu se standardy ZoKB / VoKB.

Předmět plnění (dílo) je detailně popsán v kap. 2 – Rozsah předmětu plnění.

2 ROZSAH PŘEDMĚTU PLNĚNÍ

2.1 VYMEZENÍ PŘEDMĚTU A ROZSAHU PLNĚNÍ

Rozsah plnění je následující:

#	Položka rozpočtu	Počet	Stručný popis položky
1	Bezpečnostní audit	1 soubor	Realizace bezpečnostního auditu v souladu se standardy ZoKB (VoKB), jehož součástí bude provedení analýzy rizik ve vztahu k zabezpečovaným IS a technologiím. Bezpečnostní audit posoudí soulad bezpečnostních opatření s obecně závaznými právními předpisy, vnitřními předpisy a jinými předpisy vztahujícími se k IS ZZS. Výstupy z bezpečnostního auditu budou sloužit jako jeden z podkladů pro zavedení systému řízení bezpečnosti informací o opatření k zjištěným neshodám a o relevantní doporučení vyplývající z bezpečnostního auditu.
2	Bezpečnostní politika a dokumentace	1 soubor	Vytvoření bezpečnostní dokumentace pro práci v kyberprostoru zadavatele v souladu s legislativou a best-practices.

Tabulka 2: Předmět a rozsah plnění

2.1.1 Související služby a náležitosti předmětu plnění

Součástí předmětu plnění jsou dále následující služby a náležitosti:

1. Projektové řízení realizace předmětu plnění.
2. Prezentace výstupů pro management objednatele.
3. Poskytnutí záruky min. 2 roky na dodané plnění.

2.2 POŽADAVKY NA PŘEDMĚT PLNĚNÍ

V této kapitole jsou uvedeny požadavky na předmět plnění.

2.2.1 Obecné a společné požadavky

V této kapitole jsou uvedeny obecné požadavky na požadované řešení:

#	Požadavek
Legislativa a další normy	
P.1	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.2	Soulad se Zákonem č. 181/2014 Sb., o kybernetické bezpečnosti v aktuálním znění (ZoKB) a vyhláškou Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti v aktuálním znění (VoKB).
P.3	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“- Prováděcí nařízení Komise).
P.4	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.5	Všechny výstupy budou dodány elektronicky ve formátech MS Office 2016 a vyšší a PDF.

Tabulka 3: Obecné požadavky

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

2.2.2 Bezpečnostní audit

2.2.2.1 Analýza rizik

Předmětem plnění je provedení analýzy rizik prostředí Objednatele dle ZoKB, resp. dle požadavků ustanovení bodů hlavy I a III VoKB, vypracování závěrečné zprávy z analýzy rizik s uvedenými zjištěními a doporučením nápravných opatření, včetně definice plánu zvládání rizik. Přílohou dokumentu budou záznamy z provedené analýzy prostředí Objednatele zpracované zástupci Dodavatele. Na základě zpracované analýzy dokumentace Dodavatel případně poskytne návrh úprav, nebo vytvoření dokumentace dle přílohy č. 5 VoKB. Detailní specifikace obsahu předmětu plnění díla je uvedena v následujících ustanoveních.

2.2.2.2 Zhodnocení organizačních opatření implementovaných v prostředí Objednatele

Oblast	Popis
Bezpečnostní politika a bezpečnostní dokumentace	Identifikace a analýza bezpečnostní dokumentace a provozních směrnic a postupů pro řízení rizik a bezpečnosti informací. Návrh úprav, nebo vytvoření dokumentace dle přílohy č. 5 VoKB.

Oblast	Popis
Systém řízení bezpečnosti informací	Identifikace organizačních částí, aktiv, stanoveného rozsahu a cílů systému řízení bezpečnosti informací Objednatele, jichž se systém řízení bezpečnosti informací týká.
Organizace bezpečnosti informací a bezpečnost lidských zdrojů	Identifikace rolí a odpovědností osob v procesu řízení rizik Oddělení odpovědností Informační bezpečnost v projektech. Povědomí, vzdělávání a školení bezpečnosti informací.
Řízení aktiv	Potvrzení správnosti identifikovaných a evidovaných primárních a podpůrných aktiv Validace hodnocení primárních aktiv. Validace hodnocení podpůrných aktiv. Ověření vlastníků aktiv a odpovědnost za aktiva. Potvrzení klasifikace informací a její implementace v prostředí Objednatele. Použití aktiv a životní cyklus aktiv.
Řízení rizik	Posouzení metodiky pro hodnocení rizik, včetně stanovení kritérií pro akceptovatelnost rizik. Posouzení procesu řízení a zvládání rizik, včetně identifikace způsobu určení osob tzv. vlastníků rizik pro následné zvládání rizik.
Řízení přístupu a přístupových práv	Požadavky organizace na řízení přístupu. Řízení přístupu uživatelů a jejich odpovědnost Řízení přístupu k systémům a aplikacím.
Fyzická bezpečnost pracovišť a zařízení	Politika řízení fyzické bezpečnosti
Bezpečnost provozu	Provozní postupy a odpovědnosti. Dokumentace provozních postupů. Řízení kapacit. Princip oddělení prostředí vývoje, testování a provozu. Ochrana proti malwaru. Zálohování. Logování, zaznamenávání a monitorování událostí Ochrana logů, logy o činnosti administrátorů a operátorů Správa provozního softwaru Opatření k auditu informačních systémů
Řízení změn	Ověření implementovaného procesu a postupů pro řízení změn včetně rolí a odpovědností osob v procesu

Oblast	Popis
	Postupy řízení a schvalování provozních změn
Nástroje pro řízení provozu a bezpečnosti informací	Identifikace implementovaných nástrojů pro řízení rizik a bezpečnosti informací (např. proces řízení aktiv, řízení změn, řízení přístupů, řízení incidentů atd.).
Akvizice, vývoj a údržba informačních systémů	Bezpečnostní požadavky informačních systémů Bezpečnost v procesech vývoje a podpory Politika bezpečného vývoje Postupy řízení změn systémů Data pro testování
Bezpečnost pro dodavatele a třetí strany	Bezpečnost informací v dodavatelských vztazích Bezpečnostní požadavky v dohodách s dodavateli Řízení dodávek služeb dodavatelů
Řízení a zvládání bezpečnostních incidentů	Řízení incidentů bezpečnosti informací, sběr, vyhodnocování, reakce a zlepšování procesu
Řízení kontinuity organizace	Plánování kontinuity bezpečnosti informací Implementace kontinuity bezpečnosti informací Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací Dostupnost vybavení pro zpracování informací Nástroj pro zajišťování úrovně dostupnosti informací
Soulad s interními a externími právními požadavky	Identifikace odpovídající legislativy a smluvních požadavků Ochrana záznamů Soukromí a ochrana osobních údajů Ochrana duševního vlastnictví
Přezkoumání bezpečnosti informací	Nezávislá přezkoumání bezpečnosti informací Shoda s bezpečnostními politikami a normami
Řízení technických zranitelností	Posouzení procesu a postupů pro řízení zranitelností (Vulnerability testování / Patch management / Penetrační testy informačního a komunikačního systému) Posouzení procesu implementace technických opatření pro řízení zranitelností a rizik
Organizační bezpečnostní opatření	Případně další zjištění vyplývající z analýzy realizovaných organizačních bezpečnostních opatření.

Tabulka 4: Zhodnocení organizačních opatření implementovaných v prostředí Objednatele

2.2.2.3 Zhodnocení technických opatření implementovaných v prostředí Objednatele

Provedení zhodnocení technických opatření dle ZoKB (výčet není explicitně uváděn, je součástí ZoKB a VoKB).

Přezkoumání implementace technických opatření do praxe. Technické ověření souladu implementace primárních a podpůrných aktiv dle požadavků ZKB:

1. Aplikace
2. Operační systémy
3. Síťové prvky
4. Bezpečnostní prvky
5. Fyzická bezpečnost
6. Zálohování
7. A dalších technických opatření v rozsahu bezpečnostních technických opatření dle ZoKB / VoKB.

2.2.2.4 Ostatní požadavky

Výsledkem auditu bude:

1. Zpráva z přezkoumání stávajícího prostředí Zadavatele s následujícím obsahem:
    a. Pro každé opatření bude uveden popis aktuálního stavu
    b. Zhodnocení z pohledu požadavků prováděcí vyhlášky KB (ZKB)
    c. Případné zhodnocení z pohledu „best practice“, pokud bude takovéto doporučení žádoucí.
    d. Každé opatření bude popsáno minimálně v rozsahu ½ A4.
    e. Obsahem zprávy jsou veškeré paragrafy obsažené v prováděcí vyhlášce (VoKB), tzn. Že se organizace zkoumá z pohledu organizační opatření, technických opatření i fyzické bezpečnosti.
2. Hodnocení stavu
    a. Přehledový dokument s výpočetní logikou, který bude hodnotit výsledek pro
        i. Technické role
        ii. Odděleně a s menší mírou detailu pro manažerské role
    b. Hodnocení bude provedeno jednotlivě pro každý požadavek paragrafů ZoKB
3. Obecný návrh nápravných opatření
    a. Cílem není hodnotit veškeré možné technické varianty nápravných opatření, ale určit orientační výši nákladů pro zajištění souladu se ZoKB a určit druh technologie.
4. Prezentace výsledků projektu pro projektový tým
    a. prezentace pro projektový tým a diskuze s týmem
5. Prezentace výsledků projektu pro vrcholový management

2.2.3 Bezpečnostní politika a dokumentace

ZZS KHK v současné době nemá zaveden systém řízení bezpečnosti informací (ISMS) ani zpracovanou bezpečnostní politiku ani bezpečnostní dokumentaci.

Bezpečnostní audit bude sloužit jako jeden z podkladů pro zavedení systému řízení bezpečnosti informací o opatření k zjištěným neshodám a o relevantní doporučení vyplývající z bezpečnostního auditu. Do bezpečnostní dokumentace musí být zapracovány všechny oblasti, které byly předmětem bezpečnostní analýzy a zohledněny výstupy (opatření) z bezpečnostního auditu.

Požadujeme vytvořit bezpečnostní dokumentaci pro práci v kyberprostoru zadavatele v souladu s legislativou (dle přílohy č. 5 VoKB) a best-practices.

Zohledněn musí být také doporučení pro systém řízení bezpečnosti informací dle normy ČSN ISO 27001 a na ní navazující normy ČSN ISO 27002, která je souborem doporučených opatření pro zajištění bezpečnosti informací, z této normy bude vycházet i nová směrnice NIS2.

Součástí dokumentace musí být odpovídající práva na jejich využití pro zaměstnance zadavatele a pracovníky smluvních stran.

2.3 Záruky

Objednatel požaduje záruku na veškeré dodané výstupy z realizace předmětu plnění v délce trvání minimálně 24 měsíců.

Záruka začíná běžet od okamžiku předání předmětu plnění. Veškeré opravy po dobu záruky budou bez dalších nákladů pro objednatele.

Součástí záruky je i shoda dodávaných výstupů s platnou legislativou v době předání předmětu plnění.

Max. doba na odstranění vady plnění je 30 dnů od prokazatelného oznámení dodavateli.

3 Harmonogram

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

#	Fáze	Doba trvání od zahájení	Doplňující informace
1	Zahájení realizace	0	Zahájení realizace bude ke dni účinnosti smlouvy o dílo.
2	Zpracování bezpečnostního auditu	90	Zpracování bezpečnostního auditu, projednání a schválení zjištěných výstupů.
3	Zpracování bezpečnostní politiky a dokumentace	180	Zpracování bezpečnostní politiky a dokumentace, projednání a schválení zjištěných výstupů.

Tabulka 5: Harmonogram

Doplňující informace: Pod pojmem „den“ je míněn kalendářní den.

4 Místa plnění

Realizace předmětu plnění bude probíhat v následujících místech plnění:

Místo	Adresa	Předmět realizace
Sídlo a centrální datové centrum	Hradecká 1690/2a, Hradec Králové PSČ: 500 12	Centrální datové centrum ZZS KHK – provoz části IS ZZS a souvisejících technologií. Sídlo ZZS KHK – místo předání výstupů předmětu plnění.

Místo	Adresa	Předmět realizace
Datové centrum IS ZOS ZZS KHK	Pražská 230/153z, Hradec Králové PSČ: 500 04	Datové centrum IS ZOS ZZS KHK – provoz části IS ZZS a souvisejících technologií.
Záložní datové centrum ZZS KHK	Areál LZS Fakultní nemocnice Sokolská 581 Hradec Králové PSČ: 500 12	Záložní/zálohovací datové centrum ZZS KHK – provoz části IS ZZS a souvisejících technologií.

Tabulka 6: Místa plnění

5 VÝCHOZÍ STAV

Výchozí stav pro provedení bezpečnostní analýzy a zpracování bezpečnostní politiky a dokumentace je důvěrný a v potřebném detailu bude poskytnut v rámci realizace předmětu plnění.

KONEC DOKUMENTU