Příloha č. 1: Specifikace díla

Úvod:

Jihočeský kraj je územním společenstvím občanů, kterému dle zákona č. 129/2000 Sb. mimo jiné náleží právo na samosprávu, kterou vykonává v rozsahu stanoveném v souladu s potřebami kraje. Kraj je veřejnoprávní korporací, vystupuje v právních vztazích svým jménem a nese odpovědnost z těchto vztahů vyplývající.

Jihočeský kraj v samostatné působnosti pečuje ve svém územním obvodu o komplexní rozvoj svého území a o potřeby svých občanů mimo jiné také v oblasti poskytování zdravotní péče prostřednictvím založení, resp. zřízení a zajištění provozu celé řady organizací v této oblasti. Založené, resp. zřízené organizace Jihočeského kraje a také Krajský úřad Jihočeského kraje jako jeden z orgánů kraje spadají pod aplikaci legislativy EU i národní legislativy v oblasti kybernetické a informační bezpečnosti.

Jihočeský kraj vnímá oblast kybernetické a informační bezpečnosti v oblasti poskytování služeb zdravotní péče i v oblasti veřejné správy jako zásadní. Jihočeský kraj chce problematiku kybernetické a informační bezpečnosti v této oblasti řešit centrálně a koordinovaně jak pro organizace zakládané krajem (nemocnice), organizace zřizované krajem (Zdravotnická záchranná služba), tak pro Krajský úřad Jihočeského kraje (dále též „Dotčené subjekty", případně „Zákazníci").

Cílem Jihočeského kraje je dosáhnout vysokého standardu zajištění kybernetické a informační bezpečnosti u dotčených subjektů, které poskytují služby široké veřejnosti, současně chce optimalizovat náklady (finanční, personální, …) spojené se zajišťováním služeb kybernetické a informační bezpečnosti pro dotčené subjekty. Jihočeský kraj stanovil rámec/katalog služeb (viz níže), které chce u dotčených subjektů řešit.

Za tímto účelem poptává Jihočeský kraj odborného externího zpracovatele studie proveditelnosti. Cílem studie proveditelnosti je posouzení tohoto záměru ve všech odpovídajících aspektech a variantách včetně stanovení ekonomického, organizačního, technického, legislativního a personálního rámce a přípravy podrobné strategie, časového harmonogramu a finančního plánu vedoucího k realizaci požadovaného záměru řešení služeb dle stanoveného rámce/katalogu služeb v celém jeho životním cyklu.

Předmětem plnění veřejné zakázky bude zpracování 1 souhrnné studie proveditelnosti pro všechny dotčené subjekty.

Definice dotčených subjektů:

- viz článek 3.2 smlouvy:
  - Krajský úřad Jihočeského kraje (počet zaměstnanců cca 480)
  - Zdravotnická záchranná služba Jihočeského kraje, p.o. (počet zaměstnanců cca 600)
  - Nemocnice České Budějovice, a.s. (počet zaměstnanců cca 3000)
  - Nemocnice Český Krumlov, a.s. (počet zaměstnanců cca 500)
  - Nemocnice Dačice, a.s. (počet zaměstnanců cca 70)
  - Nemocnice Jindřichův Hradec, a.s. (počet zaměstnanců cca 950)
  - Nemocnice Písek, a.s. (počet zaměstnanců cca 950)
  - Nemocnice Prachatice, a.s. (počet zaměstnanců cca 400)
  - Nemocnice Strakonice, a.s. (počet zaměstnanců cca 600)
  - Nemocnice Tábor, a.s. (počet zaměstnanců cca 1200)

Zpracování dílo bude realizováno ve 3 níže uvedených etapách:

1. **Sběr a analýza podkladů** od všech dotčených subjektů objednatele minimálně v takovém rozsahu, aby na jejím základě bylo možné kvalitní stanovení specifikace variant požadovaných služeb a bylo možné jednoznačné určení optimální varianty každé jednotlivé služby. (zhotovitel bude maximální množství práce realizovat formou osobních pohovorů/návštěv/šetření/konzultací prostřednictvím osob uvedenými v nabídce v sídle jednotlivých dotčených subjektů objednatele)
2. **Návrh variant řešení** 15 služeb definovaných níže v „katalogu služeb požadovaných zákazníky". Služby musí být navrženy modulárně, aby je bylo možné budovat a integrovat postupně do jednoho logického celku. Služby musí být rovněž navrženy jako škálovatelné. Vždy budou uvažovány min.:
   a. lokální varianta – organizace řeší sama (vlastními prostředky – technické, personální)
   b. lokální varianta – organizace řeší outsourcingem
   c. centrální varianta – nově založená organizace řeší sama (vlastními prostředky – technické, personální)
   d. centrální varianta – nově založená organizace řeší outsourcingem
3. **Výběr jedné optimální varianty** – výběr 1 optimální varianty z variant navržených v etapě 2 bude poveden ve spolupráci zhotovitele a objednatele. Zhotovitel provede odborné posouzení vybrané varianty. Výstupem studie proveditelnosti je 1 optimální varianta řešení služeb uvedených v Katalogu služeb.

Požadavky na výstupy jednotlivých etap a požadavky na obsah výsledné studie proveditelnosti:

- Analýza podkladů od všech subjektů, tzn. výstup analýzy musí být pro objednatele jednoznačný, potvrzení proběhne vzájemným odsouhlasením mezi objednatelem a zhotovitelem (bude výstupem etapy 1)
- Konkrétní technické řešení pro každou službu včetně popisu vybraného řešení a ověření shody s požadavky legislativy v oblasti kybernetické bezpečnosti a v oblasti auditu kybernetické bezpečnosti (bude výstupem etap 2, 3)

- Konkrétní forma plnění po každou službu včetně popisu kým bude daná služba realizována (založená firma, dodavatelská firma, vlastními silami, …) (bude výstupem etap 2, 3)
- Zdůvodnění vybrané formy (technické, finanční v období investiční fáze a 5 let provoz, personální, právní, …) (bude výstupem etapy 3)
- Matice řešení versus jejich čerpání dotčenými subjekty objednatele (bude výstupem etapy 3)
- Harmonogram případné realizace řešení včetně návrhu posloupnosti realizace jednotlivých kroků (bude výstupem etapy 3)
- Finanční náklady na každé řešení pro každý dotčený subjekt (pro každý dotčený subjekt můžou být náklady různé) jak v investiční fázi, tak ve fázi provozní (bude výstupem etap 2, 3)
- Možnosti financování z veřejných zdrojů včetně možnosti financování ze strukturálních fondů EU (bude výstupem etap 2, 3)

Obecné požadavky na realizaci díla v jednotlivých etapách:

- Na konci každé etapy předloží zhotovitel objednateli draft dokumentu s výsledky etapy.
- Objednatel schvaluje předložený draft s výsledky etapy:
    - při nesouhlasu s výstupem objednatel předá zhotoviteli písemně seznam připomínek a tento seznam připomínek při osobním setkání zhotoviteli představí a vysvětlí,
    - časový úsek od předání výsledků etapy zhotovitelem objednateli do okamžiku předání seznamu připomínek objednatele zhotoviteli se nezapočítává do celkové doby plnění zakázky,
    - proces připomínkování výsledků etapy probíhá do okamžiku bezvýhradní akceptace výsledků etapy objednatelem,
    - o akceptaci dokumentu s výsledky etapy bude proveden písemný zápis.
- Na konci každé etapy zajistí zhotovitel prezentaci finálního výstupu každé etapy managementu objednatele.
- Komunikace mezi zhotovitelem a objednatelem bude probíhat po celou dobu plnění minimálně 1x týdně na úrovni osobní případně online schůzky „Projektového týmu". Z této schůzky zhotovitel vždy vyhotoví nejpozději do příštího pracovního dne zápis. který bude podléhat schválení ze strany objednatele.

Pozn. Objednatel požaduje, aby součástí projektového týmu byl Auditor kybernetické bezpečnosti. Tento požadavek vychází jednak ze skutečnosti, že objednatel definuje jako jednu ze služeb v rámci „Katalogu služeb požadovaných zákazníky" zajištění role Auditora kybernetické bezpečnosti a současně z důvodu, aby zhotovitel již při návrhu jednotlivých variant (viz výstupy etap 2, 3) uvažoval i hledisko shody navrženého řešení s požadavky v oblasti legislativy a budoucího ověření shody v rámci auditů kybernetické bezpečnosti, které bude realizovat objednatel. Zkušenosti osoby v pozici Auditora kybernetické bezpečnosti se uplatní při vytváření studie proveditelnosti. Objednatel neočekává, že bude auditovat přímo provedenou studii.

Katalog služeb požadovaných zákazníky:

- **zákazník** – viz dotčené subjekty
- **poskytovatel** – organizace založená Jihočeským krajem, poskytovatel IT služeb pro zákazníky

1) Manažer kybernetické bezpečnosti:

- poskytovatel disponuje IT odborníkem/odborníky s kvalifikací Manažer kybernetické bezpečnosti:
    - vzdělání, kvalifikační předpoklady, znalosti:
        - praxe min. 3 roky v oboru informační nebo kybernetické bezpečnosti, případně absolvování studia na vysoké škole a alespoň 1 rok praxe v oboru informační nebo kybernetické bezpečnosti
        - norem ISO/IEC 27000 a obdobných norem v oblasti bezpečnosti
        - legislativy v oblasti informační a kybernetické bezpečnosti, eGovernmentu a dalších relevantních právních předpisů
        - přehled v oblasti ICT (operační systémy, databáze, aplikace, datové sítě) s důrazem na bezpečnost
        - v oblasti řízení rizik
        - v oblasti řízení kontinuity činností
    - doporučené certifikace:
        - normy řady ISO/IEC 27000
        - Certified Information Security Manager (CISM)
        - Certification in Risk and Information Systems Control (CRISC)
        - Certified Information Systems Security Professional (CISSP)
- Zákazník může čerpat tuto službu v různém rozsahu od plného outsourcingu své povinnosti/potřeby mít zřízenou pozici Manažer kybernetické bezpečnosti po ad-hoc konzultace na téma kyberbezpečnosti
- Manažer kybernetické bezpečnosti řeší kyberbezpečnost v rámci organizace poskytovatele
- Manažer kybernetické bezpečnosti řeší soulad kyberbezpečnosti služeb poskytovaných poskytovatelem se stavem kyberbezpečnosti zákazníka

2) Architekt kybernetické bezpečnosti:

- poskytovatel disponuje IT odborníkem/odborníky s kvalifikací Architekt kybernetické bezpečnosti:
    - vzdělání, kvalifikační předpoklady, znalosti:
        - praxe min. 3 roky v oboru informační nebo kybernetické bezpečnosti, případně absolvování studia na vysoké škole a alespoň 1 rok praxe v oboru informační nebo kybernetické bezpečnosti
        - norem ISO/IEC 27000 a obdobných norem v oblasti bezpečnosti

        - legislativy v oblasti informační a kybernetické bezpečnosti, eGovernmentu a dalších relevantních právních předpisů
        - v oblasti architektury informačních a komunikačních systémů a jejího navrhování (nástroje v oblasti architektury)
        - v oblasti HW, operační systémy a software
        - podnikové procesy a jejich integrace a závislost na ICT
        - řízení bezpečnosti a rizik
        - bezpečnost komunikací a sítí
        - řízení identit a přístupů
        - hodnocení a testování bezpečnosti
        - bezpečnost provozu
        - základní principy bezpečného vývoje softwaru
        - integrace a závislosti ICT a obchodních procesů
    - doporučené certifikace:
        - normy řady ISO/IEC 27000
        - CompTIA Security+
        - Certified Information Security Manager (CISM)
        - Certification in Risk and Information Systems Control (CRISC)
        - Certified Information Systems Security Professional (CISSP)
- Zákazník může čerpat tuto službu v různém rozsahu od plného outsourcingu své povinnosti/potřeby mít zřízenou pozici Architekt kybernetické bezpečnosti po ad-hoc konzultace na téma rozvoje kyberbezpečnosti
- Architekt kybernetické bezpečnosti navrhuje opatření pro zvýšení kyberbezpečnosti poskytovatele, jeho interních IT systémů a služeb poskytovaných směrem k zákazníkovi
- Architekt kybernetické bezpečnosti navrhuje opatření pro zvýšení kyberbezpečnosti poskytované poskytovatelem s ohledem na potřeby zákazníků

3) Auditor kybernetické bezpečnosti:

- poskytovatel disponuje IT odborníkem/odborníky s kvalifikací Auditor kybernetické bezpečnosti.
    - vzdělání, kvalifikační předpoklady, znalosti:
        - praxe min. 3 roky v oboru informační nebo kybernetické bezpečnosti, případně absolvování studia na vysoké škole a alespoň 1 rok praxe v oboru informační nebo kybernetické bezpečnosti
        - legislativy v oblasti informační a kybernetické bezpečnosti, eGovernmentu a dalších relevantních právních předpisů
        - procesů a postupů v oblasti interního auditu
        - metodologie a rámce auditu informační a kybernetické bezpečnosti
        - v oblasti strategického a taktického řízení ICT
        - v oblasti ochrany aktiv
    - doporučené certifikace:
        - Certified Information Systems Auditor (CISA)

        - Certified Internal Auditor (CIA)
        - Certified in Risk and Information Systems Control (CRISC)
        - Lead auditor Information Security Management System (Lead Auditor ISMS)
        - Auditor BI (akreditační schéma ČIA)
- Zákazník může čerpat tuto službu v různém rozsahu od plného outsourcingu své povinnosti/potřeby mít zřízenou pozici Auditor kybernetické bezpečnosti po ad-hoc konzultace na téma rozvoje kyberbezpečnosti
- Auditor kybernetické bezpečnosti realizuje bezpečnostní audity pro zvýšení kyberbezpečnosti poskytovatele, jeho interních IT systémů a služeb poskytovaných směrem k zákazníkovi
- Auditor kybernetické bezpečnosti realizuje bezpečnostní audity pro zvýšení kyberbezpečnosti s ohledem na potřeby zákazníků

4) Řešení pro mailovou komunikaci:

a) anti-X ochrana:

- poskytovatel poskytuje zákazníkům službu plné anti-X (anti SPAM, anti Malware, anti Phishing, Sandboxing apod.) ochrany mailové komunikace zákazníka ve směru příchozí i odchozí mailové komunikace
- poskytovaná služba je zcela nezávislá na existujícím mailovém systému zákazníka
- příchozí mailová komunikace od externích odesílatelů je směrována primárně do této služby, po prověření/označení/vyhodnocení je komunikace předána poštovnímu systému zákazníka
- obdobně služba funguje i pro mailovou komunikaci ve směru od zákazníka k externím subjektům
- při příjmu/odesílání pošty z/do Internetu služba realizuje opatření pro zabezpečení e-mailové komunikace definované v legislativě (např. SPF, DKIM, DMARC, ...)
- služba je realizována mimo IT prostředí zákazníka

b) plný outsourcing mailových služeb:

- poskytovatel poskytuje zákazníkům službu plného outsourcingu poštovních služeb
- služba outsourcingu poštovních služeb obsahuje minimálně tyto komponenty:
    - mailboxy
    - kalendáře
    - poznámky
    - úkoly
- poskytovaná služba plného outsourcingu poštovních služeb bude kompatibilní zejména s následujícími platformami/operačními systémy:
    - aplikace MS Outlook
    - iOS
    - Android

- poskytovaná služba plného outsourcingu poštovních služeb bude poskytovat uživatelské webové rozhraní pro přístup ke všem svým komponentám
- poskytovaná služba plného outsourcingu poštovních služeb bude z pohledu správy identit uživatelů plně kompatibilní a integrovaná s doménami Microsoft AD a IDM systémy zákazníka s možností automatizace životního cyklu mailboxu

5) EDR/XDR - detekce bezpečnostních incidentů na koncových zařízeních

- poskytovatel poskytuje zákazníkovi službu detekce bezpečnostních incidentů na koncových zařízeních zákazníka
- poskytovatel metodicky řídí nasazení služby do prostředí zákazníka, zejména instalaci sond na koncová zařízení zákazníka a implementaci centrální správy celého řešení do prostředí zákazníka
- poskytovatel poskytuje podporu pro celé řešení tak, aby zákazník mohl čerpat výstupy/notifikace z nasazeného řešení o detekci bezpečnostních incidentů a využít je pro řízení svého provozu a jejich mitigaci
- výstupy z celého EDR/XDR řešení jsou zároveň předávány do centrálního úložiště logů a slouží jako zdroj informací pro SOC/SIEM (viz dále)

6) Centrální úložiště logů:

- poskytovatel poskytuje službu centrálního úložiště logů
- služba je poskytována centrálně mimo IT prostředí zákazníka
- služba slouží pro sběr/uchovávání/standardizaci logů/informací z IT prostředí zákazníka a jako zdroj logů/informací pro následné vyhodnocování v SOC/SIEM (viz dále)
- poskytovatel poskytuje zákazníkovi metodickou podporu pro konfiguraci jeho IT prostředí tak, aby do centrálního úložiště logů odcházely z prostředí zákazníka relevantní logy/informace
- pokud je pro sběr logů na straně zákazníka nutné implementovat nějaké nové technické prostředky, poskytovatel poskytuje správu těchto prostředků

7) NDR - detekce bezpečnostních incidentů na síťové vrstvě:

- poskytovatel poskytuje zákazníkovi službu detekce bezpečnostních incidentů na síťové vrstvě
- poskytovatel metodicky řídí nasazení služby do prostředí zákazníka, zejména instalaci sond/zařízení pro sběr informací o provozu na síťové vrstvě v síti zákazníka
- poskytovatel ve spolupráci se zákazníkem spravuje naimplementované sondy/zařízení v síti zákazníka
- poskytovatel provozuje centrální nástroj pro vyhodnocování výstupů ze sond/zařízení umístěných v síti zákazníka a provádí vyhodnocení shromážděných informací
- výstupy z NDR systému jsou předávány do centrálního úložiště logů a slouží jako zdroj informací pro SOC/SIEM (viz dále)

8) SOC - Computer security incident response team (CSIRT):

- poskytovatel poskytuje zákazníkovi službu SOC/CSIRT v režimu 24x7x365
- poskytovatel implementuje centrální nástroj SIEM pro vyhodnocování logů uložených v centrálním úložišti logů
- poskytovatel poskytuje zákazníkovi službu SOC (Security Operations Center) v režimu 24x7x365, která (zejména) pomocí nástroje SIEM detekuje hrozby/nestandardní události v prostředí zákazníka
- poskytovatel provádí plnou analýzu zjištěných hrozeb/nestandardních událostí v prostředí zákazníka na úrovních L1, L2 a L3 - tedy detekci, posouzení a podporu pro mitigaci zjištěných skutečností
- poskytovatel notifikuje zákazníka o všech zjištěných skutečnostech včetně poskytnutí návrhů na mitigaci zjištěných událostí
- poskytovatel disponuje IT odborníkem/odborníky s kvalifikací pro výkon činnosti Computer security incident response team (CSIRT)
- poskytovatel poskytuje zákazníkovi službu CSIRT pro zvládání závažných bezpečnostních incidentů v IT prostředí zákazníka

9) off-site zálohování a disaster recovery lokalita:

- poskytovatel poskytuje zákazníkovi službu off-site zálohování a disaster recovery lokalita
- poskytovatel poskytuje zákazníkovi centrální prostředky pro realizaci off-site zálohy pořizované v prostředí zákazníka
- poskytovatel zajišťuje bezpečné uložení off-site zálohy tak, aby nemohla být modifikována ze strany prostředí zákazníka jako ochranu před znehodnocením této zálohy při výskytu kybernetického incidentu v prostředí zákazníka
- poskytovatel vyhodnocuje uložené off-site zálohy s cílem identifikovat probíhající postupné útoky na IT prostředí zákazníka
- poskytovatel poskytuje službu periodické kontroly validnosti uložených off-line záloh formou automatizovaných testovacích obnov dat
- poskytovatel poskytuje službu centrální disaster recovery lokality pro účely testování obnovy dat a IT prostředí zákazníka, provádění testování nad obnovenými daty a IT prostředím zákazníka a převedení IT provozu zákazníka do tohoto prostředí v případě závažných událostí v lokálním prostředí zákazníka
- poskytovatel poskytuje zákazníkovi metodickou podporu při vytváření disaster recovery plánů pro činnosti prováděné v disaster recovery lokalitě a testování těchto plánů

10) ochrana perimetru zákazníka a internetové komunikace:

- poskytovatel poskytuje ve spolupráci se zákazníkem zákazníkovi službu ochrana perimetru zákazníka a internetové komunikace
- poskytovatel poskytuje ve spolupráci se zákazníkem zákazníkovi službu, která povede ke zvýšení zabezpečení komunikace mezi IT prostředím zákazníka a prostředím Internetu
- služba zahrnuje ochranu perimetru zákazníka na bázi firewallu (ochrana na úrovni L3 referenčního modelu ISO/OSI)

- služba zahrnuje ochranu komunikace na bázi inspekce/kontroly jednotlivých aplikací/protokolů (ochrana na úrovni L4/L7 referenčního modelu ISO/OSI)

11) PIM/PAM nástroje:

- poskytovatel poskytuje zákazníkovi službu PIM/PAM nástroje
- poskytovatel poskytuje zákazníkovi službu implementace a správy nástroje PIM/PAM do IT prostředí zákazníka
- poskytovatel poskytuje zákazníkovi službu metodické podpory při provozování nástroje PIM/PAM

12) skenování zranitelností v IS zákazníka:

- poskytovatel poskytuje zákazníkovi službu skenování zranitelností v IS zákazníka
- poskytovatel periodicky provádí zjišťování výskytu zranitelností na perimetru i uvnitř IT prostředí zákazníka
- poskytovatel informuje zákazníka o zjištěných skutečnostech
- poskytovatel poskytuje zákazníkovi informace/postupy/konzultace k mitigaci zjištěných skutečností

13) nástroj pro provozní dohled:

- poskytovatel poskytuje zákazníkovi službu nástroj pro provozní dohled
- poskytovatel poskytuje zákazníkovi metodickou podporu pro nasazení a provoz nástroje pro provozní dohled v IT prostředí zákazníka

14) centrální nástroj pro správu KBU a KBI / Helpdesk:

- poskytovatel poskytuje zákazníkovi službu centrální nástroj pro správu KBU/KBI a Helpdesk
- poskytovatel provozuje centrální nástroj pro komunikaci se zákazníkem o všech skutečnostech vyplývajících ze služeb poskytovaných zákazníkovi
- poskytovatel řeší integraci centrálního nástroje s již existujícími nástroji typu Helpdesk v IT prostředí zákazníka

15) školení pro podporu kybernetické bezpečnosti:

- poskytovatel poskytuje zákazníkovi službu školení pro podporu kybernetické bezpečnosti
- poskytovatel zajišťuje zákazníkovi školení uživatelů/správců/managementu v oblasti kybernetické bezpečnosti