Níže uvedeného dne, měsíce a roku uzavřely smluvní strany

Klatovská nemocnice, a.s.
se sídlem Plzeňská 929, 339 01 Klatovy
IČO: 263 60 527, DIČ: CZ699005333
zapsaná v obchodním rejstříku vedeném Krajským soudem v Plzni, v oddílu B, vložka 1070
zastoupená Ing. Zdeňkem Švandou, předsedou představenstva, MUDr. Petrem Hubáčkem, MBA, LL.M., místopředsedou představenstva, Ing. Ondřejem Provalilem, MBA, členem představenstva, Ing. Michalem Filařem, členem představenstva, Mgr. Danielem Hajšmanem, členem představenstva
číslo účtu: [redacted]
(dále také „**Poskytovatel**“)

a

Zdravotnická záchranná služba Plzeňského kraje, příspěvková organizace
se sídlem Klatovská třída 2960/200i, Jižní Předměstí, 301 00 Plzeň
IČO: 45333009, DIČ: CZ45333009
zapsaná v OR vedeném Krajským soudem v Plzni, oddíl Pr, vložka 684
zastoupená MUDr. Bc. Pavlem Hrdličkou, ředitelem
(dále jen „**Objednatel**“)

tuto

smlouvu o poskytování služeb v oblasti kybernetické bezpečnosti
dle § 1746 odst. 2 občanského zákoníku, ve znění pozdějších předpisů (dále jen „**Smlouva**“)

1. Účel a předmět smlouvy

1.1 Účelem Smlouvy je využití zdrojů, know-how a organizačních schopností Poskytovatele k provádění odborných expertních a poradenských činností v oblasti kybernetické bezpečnosti a na zajištění výkonu činnosti manažera kybernetické bezpečnosti a architekta kybernetické bezpečnosti Objednatele dle Specifikace Služeb manažera kybernetické bezpečnosti a architekta kybernetické bezpečnosti, která tvoří Přílohu č. 1 této Smlouvy v souladu s vyhláškou č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, ve znění pozdějších předpisů (dále jen „**vyhláška o kybernetické bezpečnosti**“ nebo „**VKB**“) a v souladu se zákonem č. 264/2025 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „**zákon o kybernetické bezpečnosti**“ nebo „**ZKB**“) (dále jen „***Služby***“). Poskytovatel se dále na základě této Smlouvy zavazuje poskytovat i jiné expertní, konzultační a poradenské činnosti v oblasti kybernetické bezpečnosti nad rámec Služeb, přičemž takové činnosti budou vykonávány dle dohody smluvních stran na základě požadavku Objednatele (dále jen „**Ostatní Služby**“)

1.2 Předmětem Smlouvy je závazek Poskytovatele poskytovat Objednateli Služby v souladu se všemi relevantními závaznými právními předpisy, či příslušnými technickými normami, které se k danému plnění vztahují, jakož i se Smlouvou sjednanými podmínkami, a současně závazek Objednatele zaplatit Poskytovateli cenu stanovenou v čl. 2 Smlouvy za jejich řádné poskytnutí.

1.3 Specifikace Služeb, které budou Poskytovatelem poskytovány, je uvedena v Příloze č. 1 této Smlouvy. Poskytovatel bude poskytovat tato plnění po jednotlivých dílčích částech, přičemž dílčím plněním se rozumí plnění poskytnuté v rámci jednoho měsíce.

Jednotlivé části plnění dle Přílohy č. 1 této Smlouvy budou poskytovány dle plánu činností dohodnutého oběma smluvními stranami.

1.4 Manažera kybernetické bezpečnosti a architekta kybernetické bezpečnosti ve smyslu ZKB a VKB bude vykonávat v rámci poskytování Služeb za Poskytovatele zaměstnanec Poskytovatele Tomáš Šenk, který splňuje zákonné požadavky pro plnění uvedených pozic. Výkonem pozic manažera a architekta kybernetické bezpečnosti zaměstnancem Poskytovatele nedochází k žádnému dočasnému ani jinému přidělení zaměstnance Poskytovatele Objednateli ani k jinému pracovněprávnímu následku, když Tomáš Šenk bude nadále zaměstnancem Poskytovatele a bude za Poskytovatele poskytovat Objednateli Služby dle této Smlouvy. Poskytovatel je oprávněn kdykoliv změnit osobu, která bude vykonávat pozici manažera kybernetické bezpečnosti a/nebo architekta kybernetické bezpečnosti, o čemž vyrozumí Objednatele.

1.5 Poskytovatel bude Služby poskytovat na svém zařízení, Objednatel Poskytovateli zajistí přihlašovací údaje do svého počítačového systému a přístup ke sdíleným prostředkům pro bezpečnou komunikaci.

1.6 V případě urgentního požadavku Objednatele (např. kybernetický bezpečnostní incident) se Poskytovatel zavazuje reagovat nejpozději do 24 hodin od obdržení základních informací a aktivně se podílet na jeho řešení.

2. Cena a platební podmínky

2.1 Cena za poskytování Služeb dle této Smlouvy v rozsahu přílohy č. 1 této Smlouvy se sjednává jako paušální cena za kalendářní měsíc (dále jen „**Paušální cena**“) a činí 50.000,- Kč bez DPH, tj. 60.500,- Kč vč. 21% DPH.

2.2 V případě Ostatních Služeb, které nejsou zahrnuty do Paušální ceny, se smluvní strany dohodly na jednotkové ceně za 1 hodinu poskytování ostatních Služeb ve výši 700,- Kč bez DPH, tj. 847,- Kč vč. 21% DPH (dále jen „**Jednotková cena**“). Cena za plnění Ostatních služeb bude hrazena vždy zpětně za uplynulý kalendářní měsíc společně s Paušální cenou, a to ve výši součinu počtu hodin poskytování Ostatních služeb v předmětném kalendářním měsíci, který bude odsouhlasen Objednatelem, a Jednotkové ceny.

2.3 Změna Paušální nebo Jednotkové ceny sjednané v této Smlouvě je možná pouze změnou této Smlouvy.

2.4 Objednatel se zavazuje hradit cenu za plnění na základě této Smlouvy na základě faktur – daňových dokladů vystavovaných Poskytovatelem vždy za uplynulý kalendářní měsíc, ve kterém Poskytovatel v souladu s touto Smlouvou Služby a Ostatní Služby poskytoval. Poskytovatel je oprávněn vystavit fakturu nejdříve první den kalendářního měsíce následujícího po kalendářním měsíci, ke kterému se faktura vztahuje. Splatnost faktury je 30 dnů od data vystavení faktury. Poskytovatel doručí fakturu Objednateli bez zbytečného odkladu po jejím vystavení. Datum uskutečnění zdanitelného plnění je poslední den kalendářního měsíce, ke kterému se faktura vztahuje. Faktura musí splňovat veškeré náležitosti daňového a účetního dokladu stanovené právními předpisy, zejména musí splňovat ustanovení zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „ZDPH“), a musí na ní být uvedena cena, označení této Smlouvy, datum splatnosti v souladu s touto Smlouvou, jinak je Objednatel oprávněn vrátit fakturu Poskytovateli k přepracování či doplnění. V takovém případě běží nová lhůta splatnosti ode dne doručení opravené faktury Objednateli. Jestliže Poskytovatel poskytoval plnění předmětu této Smlouvy pouze po část kalendářního měsíce, je oprávněn fakturovat pouze cenu přiměřeně tomu sníženou.

2.5 Sjednané úhrady budou prováděny bezhotovostními převody z bankovního účtu Objednatele na bankovní účet Poskytovatele uvedený v záhlaví této Smlouvy. Dnem úhrady se vždy rozumí den odepsání příslušné částky z bankovního účtu Objednatele.

3. Součinnost, práva a povinnosti smluvních stran

3.1 Objednatel se zavazuje Poskytovateli poskytovat součinnost vyplývající ze Smlouvy, a to pouze v potřebném rozsahu požadovaném Poskytovatelem.

3.2 Objednatel se zavazuje Poskytovateli poskytnout veškeré doklady, písemnosti, dokumentaci a informace nezbytné pro plnění předmětu Smlouvy.

3.3 Objednatel se zavazuje umožnit Poskytovateli přístup v nezbytně nutném rozsahu do objektů ve vlastnictví nebo užívání Objednatele a k technickým prostředkům v rozsahu nezbytném pro plnění předmětu této Smlouvy.

3.4 Poskytovatel je povinen postupovat při plnění předmětu Smlouvy s odbornou péčí, podle nejlepších znalostí a schopností a sledovat a chránit oprávněné zájmy Objednatele. Dále je povinen postupovat v souladu s pokyny Objednatele a jeho interními předpisy, které souvisí s předmětem plnění Smlouvy a k nimž Objednatel Poskytovateli zajistí přístup.

3.5 Poskytovatel se zavazuje informovat Objednatele o všech skutečnostech majících vliv na plnění této Smlouvy.

3.6 Poskytovatel je povinen v průběhu poskytování Služeb neprodleně upozornit Objednatele na nevhodnost jeho pokynů nebo předané dokumentace. Toto upozornění musí mít písemnou formu. V takovém případě je Objednatel povinen se k tomuto upozornění bez zbytečného odkladu písemně vyjádřit a je povinen učinit veškerá opatření, aby Poskytovatel mohl pokračovat v poskytování Služeb řádně a včas.

3.7 Objednatel se zavazuje informovat provozovatele systémů o skutečnosti, že roli Manažera kybernetické bezpečnosti a Architekta kybernetické bezpečnosti vykonává jím určená osoba (ke dni uzavření této Smlouvy je takovou osobou za Poskytovatele Tomáš Šenk) a je tak oprávněna činit veškeré kroky vyplývající ze ZKB, VKB a této Smlouvy, a to i ve vztahu k ostatním provozovatelům.

3.8 Objednatel je oprávněn kdykoliv kontrolovat provádění smluvní činnosti Poskytovatele. Zjistí-li, že Poskytovatel realizuje povinnosti vyplývající ze Smlouvy v rozporu s povinnostmi stanovenými obecně závaznými právními předpisy nebo Smlouvou, je oprávněn požadovat, aby Poskytovatel bezplatně a bezodkladně odstranil vady vzniklé z této činnosti a činnost prováděl řádným způsobem.

4. Zajištění důvěrnosti předávaných dat

4.1 Poskytovatel je povinen při užívání a čerpání jakýchkoli informací, dat, podkladů, zejména o cílech a smluvním vztahu k veřejné zakázce a jejího plnění, informačních systémech, personálním zabezpečení, vnitřní struktuře organizace a o skutečnostech, které se vztahují k bezpečnostním a technickým opatřením, kdy se stává příjemcem a uživatelem těchto informací, jako chráněných informací, ve smyslu ustanovení § 1730 občanského zákoníku, dodržovat zákonné předpisy pro oblast kybernetické bezpečnosti, interní předpisy a počínat si při svém jednání tak, aby nedocházelo k porušování bezpečnostních opatření, nebyla snižována a poškozována bezpečnostní image Objednatele a důvěryhodnost těchto zdrojů a nedošlo k neoprávněnému zásahu do sítí a informačních systémů s následkem jejich poškození.

4.2 Poskytovatel se zavazuje, že:

a) Žádné informace získané od Objednatele nebude poskytovat třetím osobám.

b) Informace a s nimi získané know-how bude používat pouze pro účely plnění povinností dle této Smlouvy, nikoli pro vlastní potřebu, výrobu, nebo pro dodávky konkurentům Objednavatele.

c) Informace zpřístupní pouze omezenému okruhu pracovníků Poskytovatele, kteří jsou určení k plnění povinností.

d) Učiní vhodná opatření a zajistí, aby pracovníci Poskytovatele udržovali v tajnosti informace Objednatele ve stejném rozsahu jako Poskytovatel a používali je pouze pro účely plnění povinností dle této Smlouvy.

e) Všechny Objednatelem poskytnuté podklady včetně materiálů, náčrtků a vzorků zůstávají výhradním vlastnictvím Objednatele. Poskytnuté podklady nesmí být Poskytovatelem rozmnožovány a musí s nimi být nakládáno tak, jako by byly označovány jako důvěrné.

4.3 Poskytovatel bere na vědomí, že zákonem určený správní orgán je oprávněn vykonávat kontrolu a dohled nad dodržováním ustanovení v oblasti kybernetické bezpečnosti a smluvní strany jsou povinny být součinné v případě výkonu státního dohledu a při provádění auditů procesu.

5. Vlastnické právo, nebezpečí škody na věci, práva duševního vlastnictví

5.1 Vlastnické právo ke všem hmotným součástem plnění předmětu Smlouvy předaným Poskytovatelem Objednateli v souvislosti s plněním předmětu Smlouvy přechází na Objednatele dnem jejich předání Objednateli.

5.2 Nebezpečí škody na všech hmotných součástech plnění předmětu Smlouvy předaných Poskytovatelem Objednateli v souvislosti s plněním předmětu Smlouvy přechází na Objednatele dnem jejich předání Objednateli.

5.3 Pokud je výsledkem činnosti Poskytovatele podle Smlouvy plnění, které naplňuje znaky díla ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, poskytuje Poskytovatel Objednateli a Objednatel od Poskytovatele získává veškerá práva související s ochranou duševního vlastnictví vztahující se k takovému dílu, a to v rozsahu nezbytném pro řádné užívání takového díla Objednatelem po celou dobu trvání příslušných autorských práv. Objednatel zejména nabývá od Poskytovatele dnem poskytnutí autorského díla Objednateli (nejpozději však ke dni podpisu protokolu o předání a převzetí Služeb dle Smlouvy, jichž je takové autorské dílo součástí) veškerá majetková práva.

5.4 Objednatel je oprávněn pořizovat pro vlastní potřebu rozmnoženiny veškeré dokumentace předané Poskytovatelem v listinné i elektronické podobě a používat text veškerých dokumentací předaných Poskytovatelem pro přípravu dalších technických dokumentací a uživatelských příruček.

5.5 Poskytovatel je povinen zajistit, aby výsledkem jeho plnění nebo jakékoliv jeho části nebyla porušena práva třetích osob. Pro případ, že užíváním předmětu plnění nebo jeho dílčí části nebo prostou existencí předmětu plnění nebo jeho dílčí části budou v důsledku porušení povinností Poskytovatele dotčena práva třetích osob, nese Poskytovatel vedle odpovědnosti za takovéto vady plnění i odpovědnost za veškeré škody, které tím Objednateli vzniknou.

6. Doba trvání a zánik Smlouvy

6.1. Smlouva se uzavírá na dobu neurčitou.

6.2. Kterákoliv ze smluvních stran je oprávněna tuto Smlouvu písemně vypovědět z jakéhokoliv důvodu nebo bez uvedení důvodu s výpovědní dobou 3 měsíce, která počne běžet od prvního dne měsíce následujícího po doručení písemné výpovědi druhé smluvní straně.

6.3. Poskytovatel je oprávněn písemně vypovědět tuto smlouvu bez výpovědní doby v případě prodlení Objednatele se zaplacením ceny za plnění dle této Smlouvy o více než 30 kalendářních dnů, když v takovém případě tato Smlouva zaniká dnem doručení písemné výpovědi Objednateli.

6.4. V případě ukončení této Smlouvy je Poskytovatel povinen předat Objednateli veškerá data a dokumentaci z plnění dle této Smlouvy nejpozději ke dni ukončení Smlouvy.

7. Závěrečná ustanovení

7.1. Smlouva může být doplňována a měněna pouze písemnými v řadě číslovanými dodatky, jakákoliv jiná forma změny je vyloučena, pokud se smluvní strany písemně nedohodnou jinak.

7.2. Smlouva se uzavírá v elektronické podobě.

7.3. Tato Smlouva se řídí právním řádem České republiky, zejména zák. č. 89/2012 Sb., občanským zákoníkem, v platném znění.

7.4. Smluvní strany se zavazují, že budou jednat vždy ve prospěch této Smlouvy, a to jak vůči sobě navzájem, tak i třetím osobám. Smluvní strany se rovněž zavazují zdržet takového jednání, které by mohl být druhou stranou vykládáno jako jednání směřující proti smyslu a účelu této Smlouvy.

7.5. Pokud pozbude některé ustanovení této Smlouvy platnosti, nemá to vliv na platnost Smlouvy jako celku. Smluvní strany se zavazují takové ustanovení nahradit novým platným, které se bude co nejvíce blížit původnímu a bude v souladu s původní vůlí stran a účelem Smlouvy.

7.6. Strany si Smlouvu přečetly, prohlašují, že byla sepsána na základě pravdivých údajů a že jim nejsou známy žádné skutečnosti bránící uzavření Smlouvy a plnění povinností z ní vyplývajících. Na důkaz souhlasu se zněním Smlouvy strany připojují své podpisy.

7.7. Smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem zveřejnění v registru smluv dle zákona č. 340/2015 Sb., o registru smluv ve znění pozdějších předpisů.

Příloha č. 1: Specifikace Služeb manažera kybernetické bezpečnosti a architekta kybernetické bezpečnosti

Poskytovatel:

[redacted]

Klatovská nemocnice, a.s.

[redacted]

Klatovská nemocnice, a.s.

Objednatel:

[redacted]

Zdravotnická záchranná služba Plzeňského kraje, příspěvková organizace
MUDr. Bc. Pavel Hrdlička
ředitel

Příloha č. 1: Specifikace Služeb manažera kybernetické bezpečnosti a architekta kybernetické bezpečnosti

Práva a povinnosti manažera kybernetické bezpečnosti a architekta kybernetické bezpečnosti

Manažer kybernetické bezpečnosti (dále jen „MKB“) odpovídá za systém řízení bezpečnosti informací v rámci organizace a je hlavním výkonným řídícím prvkem systému řízení informační bezpečnosti. Je oprávněn jednat za organizaci ve věcech základních povinností kybernetické bezpečností (dále jen „ZKB“). Mezi jeho klíčové povinnosti patří:

a. odpovědnost za řízení systému řízení bezpečnosti informací,

b. navrhování koncepce systému řízení bezpečnosti informací,

c. pravidelná komunikace a poskytování informací vrcholovému vedení organizace,

d. předkládání Zpráv o hodnocení aktiv a rizik, Plánu zvládání rizik a Prohlášení o aplikovatelnosti Výboru řízení kybernetické bezpečnosti (dále jen „VŘKB“),

e. předkládat zprávu o přezkoumání SŘBI VŘKB,

f. spolupráce s ostatními osobami zastávajícími bezpečnostní role,

g. poskytování pokynů pro zajištění bezpečnosti informací při vytváření, hodnocení, výběru, řízení a ukončení dodavatelských vztahů v oblasti informačních a komunikačních technologií,

h. spolupráce s NÚKIB (hlášení kontaktních údajů, hlášení bezpečnostních incidentů, spolupráce při šetření, zaslání reaktivních opatření apod.),

i. bez zbytečného odkladu informování MKB IS o reaktivních a ochranných opatřeních vydaných NÚKIB,

j. vedení evidence osob určených do bezpečnostních rolí,

k. podílení se na procesu řízení rizik,

l. koordinace řízení incidentů (komunikace s GovCERT/CSIRT apod.),

m. vyhodnocování vhodnosti a účinnosti bezpečnostních opatření,

n. navrhování provedení kontrol dodržování bezpečnostní politiky,

o. koordinace činnosti VŘKB, příprava podkladů k jednání a předkládání návrhů ochranných opatření k projednání,

p. předkládání žádostí o výjimky VŘKB a vedení evidence schválených výjimek; pravidelně min. 1x za rok provádění revize požadavků na jejich trvání, u dočasných výjimek provádění revize požadavku nejpozději ke dni ukončení platnosti výjimky,

q. zohledňování požadavků vyplývajících z organizačních a technických bezpečnostních opatření při výběru dodavatelů, a to v míře nezbytné pro splnění ZKB a vyšších povinností kybernetické bezpečnosti (dále jen „VKB“),

r. vedení evidence primárních aktiv resortu.

Práva MKB jsou

a. zajistit splnění požadavků ZKB a VKB a vyžadovat součinnost a plnění úkolů od osob určených do bezpečnostních rolí a VŘKB,

b. vyžadovat od NÚKIB (GovCERTu) metodickou podporu a pomoc,

c. vyžadovat součinnost NÚKIB (GovCERT) aj. CSIRT při výskytu kybernetického bezpečnostního incidentu či události,

d. vypisovat výběrová řízení na zajištění provedení auditů kybernetické bezpečnosti,

e. spolupracovat s externími subjekty na zajištění kybernetické bezpečnosti,

f. schvalovat žádosti o výjimky z pravidel stanovených bezpečnostními politikami a vyžadovanými ZKB a VKB, případně tyto žádosti eskalovat na VŘKB.

Architekt kybernetické bezpečnosti (dále jen „AKB“) odpovídá za zajištění návrhu implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura informačního a komunikačního systému.
Mezi jeho klíčové povinnosti patří

a. znalost ZKB, jeho prováděcích vyhlášek a souvisejících předpisů,

b. definovat bezpečnostní požadavky na návrh, vývoj, testování a implementaci IS a změnu stávajících bezpečnostních požadavků,

c. zajišťovat bezpečnostní architekturu s cílem zajištění bezpečnosti primárních aktiv, tj. jejich důvěrnosti, dostupnosti a integrity, a to konkrétně

1. posuzovat zajištění bezpečnosti prvků, které tvoří podpůrná aktiva ve vazbě na primární aktiva,

2. určovat klíčové podmínky, principy a modely architektury IS, posuzovat a vybírat technologie a stanovovat koncepci bezpečnostního rozvoje IS;

3. řídit, koncepčně vést a schvalovat bezpečnostní architekturu informačních a komunikačních systémů včetně podpůrných technických aktiv,

4. definovat požadavky na nástroje pro zajištění technických opatření kybernetické bezpečnosti,

5. vytvářet a udržovat model architektury kybernetické bezpečnosti (procesní model, aplikační architekturu, technologie atd.),

6. navrhovat změny architektury kybernetické bezpečnosti,

7. analyzovat úroveň architektury kybernetické bezpečnosti.

d. předkládat návrh implementace bezpečnostních opatření,

e. vytvářet testovací postupy a odpovídající kritéria akceptace,

f. navrhovat a optimalizovat opatření a procesy řešení bezpečnostních událostí a incidentů,

g. spolupracovat a předkládat návrhy změn bezpečnostní politiky a bezpečnostních dokumentů,

h. dohlížet na implementaci bezpečnostních opatření,

i. ve spolupráci s manažerem IS navrhovat opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu,

j. provádět kontroly, hodnocení a testování funkčnosti zavedených bezpečnostních opatření,

k. poskytovat součinnost dalším bezpečnostním rolím,

l. spolupracovat na zajištění trvalé ochrany aplikací a informací IS dostupných z vnější sítě,

m. spolupracovat při aplikaci používání kryptografických prostředků a systému správy klíčů.

Odpovědností AKB je

a. příprava návrhu implementace bezpečnostních opatření pro snižování rizik, příprava pravidel a standardů pro oblast kybernetické bezpečnosti,

a. návrh a výběr nástrojů pro zajištění technických opatření kybernetické bezpečnosti

b. definice klíčových projektů, které vedou k naplnění bezpečnostní politiky a k cílovému stavu architektury kybernetické bezpečnosti a dohled nad jejich realizací a vyhodnocením,

c. analýza úrovně architektury kybernetické bezpečnosti, definice metrik a identifikace existujících rizik a návrh strategie na zmírnění rizik,

d. vytváření plánů implementace architektury kybernetické bezpečnosti ČÚZK a podřízených organizací,

e. předkládat návrhy opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu nebo události,

f. předkládat návrhy opatření a procesy řešení bezpečnostních událostí a incidentů,

g. spolupracovat na zajištění trvalé ochrany aplikací a informací dostupných z vnější sítě,

h. poskytovat součinnost dalším bezpečnostním rolím.

Součást této činnosti tvoří architektonické návrhy

a. informačních a komunikačních systémů,

b. hardwarových komponent, nástrojů,

c. operačních systémů a software,

d. bezpečnosti komunikací a sítí,

e. pro řízení identit a přístupů.

Mezi jeho další povinnosti náleží

a. účast při řízení bezpečnosti a rizik,

b. účast při hodnocení a testování bezpečnosti,

c. posouzení a hodnocení bezpečnosti provozu,

d. stanovení zásad a principů bezpečného vývoje software,

e. hodnocení integrace a závislosti ICT a obchodních procesů.

Služby MKB a AKB musí zahrnovat:

- Spolupráce na probíhajících programech a projektech, uvedených v bezpečnostní dokumentaci, která bude Dodavateli předána po nabytí účinnosti Smlouvy v oblasti kybernetické bezpečnosti ve všech jejich fázích. Řízení prací při tvorbě vstupních analýz předmětů a cílů programů k řízení bezpečnosti informací.
- Vyřizování operativních dotazů oprávněných osob projektu směrem ke kybernetické bezpečnosti.
- Spolurozhodování a součinnost v zadávacích řízeních a při smluvním zabezpečení programů a projektů v oblasti kybernetické bezpečnosti, zahrnujících zejména veřejné zakázky na dodávky Významných dodavatelů dle VKB, spolupráci na hodnocení dodavatelů spojených s řízením dodavatelů dle VKB.
- Účast na projektových jednáních a Výboru pro řízení kybernetické bezpečnosti měsíce.
- Řízení a koordinace bezpečnostní dokumentace, zahrnující implementaci organizačních a technických opatření v návaznosti na prováděné kontroly, audity.
- Spolurozhodování o časových plánech realizace programů v oblasti kybernetické bezpečnosti.
- Koordinaci postupů a řízení projektových týmů v oblasti kybernetické bezpečnosti.
- Vedení a spolurozhodování při řízení rizik a příležitostí v programech a projektech.
- Vedení a spolurozhodování při řízení kvality programů a projektů.
- Vrcholová kontrola výstupů z programů a projektů v části kybernetické bezpečnosti.
- Vrcholová kontrola kompletní dokumentace programů a projektů.
- Vedení a spolurozhodování při řízení změn v programech a projektech.
- Vedení a spolurozhodování při reportování stavu realizace programů a projektů k řízení bezpečnosti informací k týmu projektových manažerů a zadavatelů projektů.
- Podílení se na rozvoji bezpečnostního povědomí o možných kybernetických hrozbách.
- Sledování změn právních předpisů v oblasti kybernetické bezpečnosti a souvisejících zákonů a navrhování změn interních předpisů.

Konkrétní činnosti vykonávané manažerem kybernetické bezpečnosti jsou minimálně v rozsahu:

- Návrh koncepce a integrace systému řízení bezpečnosti informací a podílení se na jeho zavádění.
- Vyhodnocení integrace systému řízení bezpečnosti do interních procesů.
- Navrhování kontrol dodržování bezpečnostních politik.

- Návrh a realizace průběžných kontrol a kontrola dodržování bezpečnostních opatření kybernetické bezpečnosti.
- Dohled nad implementací opatření kybernetické bezpečnosti.
- Vyhodnocování monitorovaných bezpečnostních ukazatelů a návrh dalších případných postupů.
- Podílení se na koordinaci řízení kontinuity činností, koordinaci řízení změn.
- Podílení se na procesu řízení rizik, koordinaci řízení bezpečnostních událostí a incidentů (komunikace s GovCERT/CSIRT, NÚKIB apod.), vyhodnocování vhodnosti a účinnosti bezpečnostních opatření.
- Konzultace s garanty informačních aktiv a vyhodnocení stavu projektů z pohledu kybernetické bezpečnosti.
- Plánování penetračních testů nebo testů zranitelnosti na základě prováděné analýzy rizik.
- Součinnost pro garanty aktiv při vyhodnocování dodavatelů z pohledu kybernetické bezpečnosti.
- Aktivní účast na projektových poradách v souvislosti s kybernetickou bezpečností a při řízení provozu.
- Aktivní účast na jednáních Výboru pro řízení kybernetické bezpečnosti.
- Spolupráce při auditech kybernetické bezpečnosti, komunikace s auditorem, zpracování a vyhodnocení zprávy od auditora kybernetické bezpečnosti a projednání stanovisek k jednotlivým požadavkům kybernetické bezpečnosti.
- Spolupráce s ostatními osobami zastávajícími bezpečnostní role, metodická pomoc při zpracování bezpečnostní dokumentace pro garanty aktiv, a konzultace a podpora v oblasti personální bezpečnosti.
- Spolupráce při přípravě a realizace školení v oblasti kybernetické bezpečnosti a průběžném vzdělávání (vzdělávání na základě bezpečnostních incidentů a auditů).
- Součinnost při zpracování Zpráv o hodnocení aktiv a rizik, Plánu zvládání rizik a Prohlášení o aplikovatelnosti a další bezpečnostní dokumentace IS.
- Vytvoření zprávy o přezkoumání SŘBI.
- Navrhování způsobu likvidace dat a vyhodnocení provedení.

K předmětu plnění Objednatel dále uvádí, že jednotlivé IS poskytující regulované služby nemají zpracovány samostatné bezpečnostní politiky (dokumentaci) ve VKB uvedených oblastech, ale jsou pro všechny IS v resortu.
V tabulkách níže je uveden podrobný rozpis činností podle čl. I odst. 1 písm. a) - c) včetně této Smlouvy, forma požadovaného výstupu a u činností podle čl. I. odst. 1 písm. c) této Smlouvy i čtvrtletí, ve kterém bude tato činnost požadována. Podrobný rozpis je uveden v návaznosti na výčet povinností MKB a AKB uvedených výše.
Lhůty pro vybrané činnosti, uvedené v tabulkách níže, požaduje Objednatel takto:

- pro pravidelné projektové schůzky s metodikem bezpečnosti (1x za 14 dní):
    - Zaslání programu 2 pracovní dny předem

- Návrh zápisu ze schůzky do 3 pracovních dní

- pro pravidelné schůzky s MKB IS a VŘKB:
  - Zaslání programu a dokumentů k jednání 4 pracovní dny předem
  - Návrh zápisu ze schůzky do 5 pracovních dní

- vyjádření k výjimce SŘBI, stanovisku k požadavkům KB, jiné konzultace do 5 pracovních dní
- stanovení bezpečnostních požadavků na významného dodavatele, řízení dodavatelů, řízení změn a obdobných stanovisek do 10 pracovních dní

- zahájení součinnosti s NÚKIB a GovCERT do 2 pracovních dní

- zahájení součinnosti při řešení kritického bezpečnostního incidentu (dále jen „KBI“) do 3 hodin od nahlášení

A. **Průběžné služby manažera a architekta kybernetické bezpečnosti**		
Ozn.	**Popis činnosti**	**Výstup**
A1	Komunikace s NÚKIB, GovCERT	Konzultace
A2	Komunikace s auditorem KB	Konzultace
A3	Komunikace s MKB IS	Konzultace
A4	Komunikace s metodikem bezpečnosti	Konzultace
A5	Komunikace s Manažerem kontinuity a CSIRT ČÚZK	Konzultace
A5	Projednání stanovisek k jednotlivým požadavkům KB	Konzultace
A6	Průběžná komunikace s Vedením o kybernetické bezpečnosti	Konzultace
A7	Konzultace s garanty informačních aktiv	Konzultace
A8	Konzultace a podpora personální bezpečnosti	Konzultace
A9	Návrh integrace systému řízení bezpečnosti do interních procesů	Návrh změn předpisů
A10	Součinnost při řešení KBI	Součinnost
A11	Jednání s dalšími MKB IS a Garanty	Zápis z jednání
A12	Jednání VŘKB	Zápis z jednání
A13	Projektová jednání 1x za 14 dní	Zápis z jednání
A14	Součinnost při kontrolách bezpečnosti	Součinnost
A15	Součinnost při komunikaci s NÚKIB	Reakce na opatření NÚKIB
A16	Pravidelné zasílání hrozeb a zranitelností a součinnost vyhodnocování dopadů	Zápis a konzultace
A17	Proaktivní a průběžné návrhy v oblasti bezpečnosti	Zápis

B. **Služby manažera a architekta kybernetické bezpečnosti**		
Ozn.	**Popis činnosti**	**Výstup**
B1	Příprava školení a průběžné vzdělávání (vzdělávání na základě incidentů a auditů)	Příprava školících materiálů, proškolení
B2	Vyhodnocení auditních zpráv KB	Stanovení nápravných opatření
B3	Vyhodnocení realizace nápravných opatření z auditních zpráv	Zpráva
B4	Vyhodnocení plnění úkolů SŘBI	Zpráva
B5	Rozvoj bezpečnostního povědomí o možných hrozbách pro uživatele, desatero bezpečnosti	Informační mail
B6	Řízení přístupů	Zpráva
B7	Řízení kontinuity činností	Zpráva
B8	Jednání MKB a MKB IS	Zápis z jednání
B9	Jednání Výboru pro řízení kybernetické bezpečnosti	Zápis z jednání
B10	Řízení dodavatelů	Stanovení bezpečnostních požadavků akvizic Konzultace k veřejným zakázkám Požadavky na hodnocení dodavatelů Součinnost při hodnocení plnění bezpečnostních opatření
B11	Řízení provozu a komunikací	Konzultace a návrhy změn procesů
B12	Řízení změn	Vyjádření k rizikům významné změny a dopadům do bezpečnosti
B13	Revize a návrh zajištění bezpečnosti komunikačních sítí	Konzultace
B14	Konzultace návrhů technických opatření	Konzultace, návrh technických parametrů
B15	Návrhy technických a organizačních opatření	Zpráva
B16	Vyhodnocení výjimek SŘBI	Zpráva

Ozn.	**Popis činnosti**	**Výstup**
C1	Řízení aktiv a rizik	Analýza rizik resortu, Plán zvládání rizik
C2	Vyhodnocení řízení nápravných opatření	Zpráva
C3	Kontrola, vyhodnocení a návrh změn řízení přístupů	Zpráva
C4	Kontrola, vyhodnocení a návrh změn řízení kontinuity	Zpráva
C5	Zpráva o přezkoumání SŘBI pro Vedení úřadu na podkladě vyhodnocených výkonnostních ukazatelů	Zpráva
C6	Stanovení plánů kontinuity	Plán kontinuity

C7	Návrh plánu vzdělávání	Plán vzdělávacích akcí
C8	Revize bezpečnostní dokumentace a návrh plánu její aktualizace	Zpráva o revizi
C9	Vyhodnocení a návrh změn likvidace aktiv	Zpráva
C10	Návrh průběžných kontrol/dodržování bezpečnostních opatření KB	Plán kontrol
C11	Vyhodnocování monitorovaných bezpečnostních ukazatelů a návrh dalších případných postupů	Zpráva
C12	Vyhodnocení KBU a návrhy změn zaznamenávaných událostí	Zpráva
C13	Plánování penetračních testů nebo testů zranitelností pro další období	Plán testů
C14	Zhodnocení výsledků penetračních testů a testů zranitelností z předchozího období	Zpráva
C15	Vyhodnocení řízení významných dodavatelů	Zpráva