**RÁMCOVÁ DOHODA**

**Objednatel:**

**MMN, a.s.**

Se sídlem: Metyšova 465, Jilemnice, 514 01

Jednající: MUDr. Jiří Kalenský, předseda představenstva a Ing. et. Ing. Imrich Kohút, člen představenstva

IČO: 05421888

DIČ: CZ 05421888

Bankovní spojení: Komerční banka, a.s. expozit. Jilemnice, č.ú. 115-34 53 310 267 / 0100

Zapsaná v obchodním rejstříku vedeném u Krajského soudu v Hradci Králové, sp. zn. B vložka 3506 (dále jen jako „Objednatel“)

**a**

**Dodavatel: invitech.cz s.r.o.**

Se sídlem: Klapálkova 2246/17, 149 00 Praha 4

Jednající: Ing. Martin Vaňko, jednatel

IČO: 02707349

DIČ: CZ02707349

Bankovní spojení: XXXXXXXXXXXXXX

zapsána v Obchodním rejstříku vedeném u Městského soudu v Praze, spisová značka: C 222845

(dále jen jako „Dodavatel“)

(Objednatel a Dodavatel dále rovněž jen jako „Smluvní strany“)

1. **PREAMBULE**
2. Objednatel jako veřejný zadavatel provedl v souladu s vnitřním organizačním předpisem zadavatele výběrové řízení na uzavření této Rámcové dohody.
3. Nabídka Dodavatele (dále jen „Nabídka“) byla vybrána jako nejvhodnější. Tato Rámcová smlouva je uzavřena s jediným vybraným Dodavatelem.
4. Obě smluvní strany prohlašují, že jsou způsobilé k právním úkonům a po vzájemném projednání a shodě uzavírají v souladu s ustanovením § 2085 a následujících zákona
č. 89/2012 Sb., občanského zákoníku, tuto smlouvu.
5. **PŘEDMĚT RÁMCOVÉ DOHODY**
6. Účelem této Rámcové dohody je vymezení základních smluvních podmínek pro vystavování následných objednávek, jejichž předmětem bude výkon role Manažera kybernetické bezpečnosti pro MMN, a.s.
7. Předmětem plnění dle této smlouvy je poskytování outsourcingu role manažera kybernetické bezpečnosti, čímž se pro účely této smlouvy rozumí zajišťování výkonu role manažera kybernetické bezpečnosti v souladu s požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti a vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti) externistou.
8. Pod pojmem výkon role Manažera KB, se rozumí zejména:
	1. **Všeobecné práva a odpovědnosti:**
* Aktivně se seznamuje a řídí všemi interními normativními akty (směrnicemi, nařízeními, metodikami atp.), které spadají do jeho působnosti.
* Řádně hospodaří se svěřenými finančními, technickými a personálními prostředky tak, aby nedocházelo ke škodám, ztrátám či zneužití majetku organizace. Dbá na efektivní a účelné vynakládání zdrojů.
* Je povinen zachovávat mlčenlivost o všech skutečnostech, s nimiž se při výkonu své funkce seznámí, a chránit citlivé či důvěrné informace před neoprávněným přístupem.
	1. **Pravomoc a odpovědnosti**

**Zodpovídá za:**

* Strategické plánování, koordinaci a dohled nad implementací kybernetických bezpečnostních opatření.
* Analýzu a vyhodnocení kybernetických rizik, přičemž navrhuje opatření ke zmírnění identifikovaných rizik.
* Spolupráci s odborníky a dodavateli při tvorbě a aktualizaci bezpečnostních standardů, postupů a pravidel.
* Vytváření, přípravu a koncepční plánování projektů a opatření kybernetické bezpečnosti. V součinnosti s představenstvem a dalšími útvary formuluje cíle a priority v oblasti kybernetické ochrany.
* Řízení a průběžný rozvoj systému řízení bezpečnosti informací (ISMS). Od počáteční analýzy rizik až po vyhodnocení kybernetických incidentů koordinuje aktivity tak, aby odpovídaly legislativním požadavkům a strategickým cílům organizace.
* Schvalování rozsahu a plánování technických opatření, která následně realizuje AKB. Sleduje průběh implementace a vyhodnocuje výsledky. Je zodpovědný za to, že AKB má k dispozici potřebné informace, zadání a součinnost k naplňování schválených projektů.
* Dodržování relevantních právních předpisů (např. zákon o kybernetické bezpečnosti
a související vyhlášky) a dbá na to, aby předpisy ukládané dozorovými orgány (NÚKIB aj.) byly řádně implementovány.
* Organizaci procesu pravidelného mapování aktiv a jejich zranitelností. Na základě průběžných analýz navrhuje bezpečnostní projekty, navrhuje změny v opatřeních
a předkládá je vedení společnosti či představenstvu k rozhodnutí.
* Ve spolupráci s AKB, ICT i dalšími organizačními jednotkami (např. dodavatelskými firmami či garanty klíčových aktiv) zodpovídá za technické, organizační a procesní kroky, které vedou k ochraně informačních systémů a k minimalizaci kybernetických rizik.
* Spolupráci s dodavateli informačních systémů a přednosty jednotlivých součástí MMN při implementaci opatření pro zmírnění kybernetických rizik u technických
a programových prostředků informačních technologií MMN.
* Stanovování a kontrolu požadavků v zadávacích dokumentacích z hlediska kybernetické bezpečnosti. Vyžaduje, aby vyhlašované veřejné zakázky (včetně zakázek malého rozsahu) obsahovaly odpovídající bezpečnostní podmínky, standardy a hodnotící kritéria. V rámci přípravy zadávacích dokumentací MKB vyhodnocuje, zda požadované funkce a parametry systémů či služeb odpovídají bezpečnostním potřebám organizace. Navrhuje případné úpravy tak, aby se minimalizovala kybernetická rizika.
* V případě projektů týkajících se informačních systémů, z pohledu kybernetické bezpečnosti:
	1. zodpovídá za zajišťování konzultace k organizaci kontrol etap dílčího plnění,
	2. rozhoduje o přípravě testovacích dat a organizaci bezpečnostního testování,
	3. informuje AKB o zkušebním a ověřovacím provozu a zátěžových testech,
	4. podílí se na přípravě a organizaci akceptačního řízení.

**Zajišťuje:**

* Proces řešení kybernetických bezpečnostních události, nebo kybernetických incidentů
a předkládá vedení MMN návrhy na způsob jejich řešení.
* Zajišťuje pravidelný bezpečnostní monitoring a testování (zátěžové testy, penetrační testy, testy odolnosti atp.) a vyhodnocuje jejich výsledky. Ve spolupráci s AKB a ICT zprostředkovává přípravu testovacích dat a koordinuje organizaci samotného testování.
* Zajišťuje v součinnosti s AKB a ICT oddělením postupy pro zvládání a eliminaci dopadů kybernetických incidentů, včetně komunikace s dotčenými subjekty (NÚKIB, vedení organizace a další).
* Schvalování technických návrhů realizace kybernetické bezpečnosti vytvořené AKB.
* Navrhuje program interních auditů v oblasti kybernetické bezpečnosti a provádí kontroly zaměřené na to, zda jsou zavedená opatření skutečně dodržována a zda odpovídají přijatým standardům.
* Spravuje veškerou dokumentaci vztahující se k řízení kybernetické bezpečnosti (směrnice, metodiky, reporty k rizikům, záznamy o incidentech apod.) a dohlíží na její aktualizaci.
* Provádění školení a informování zaměstnanců o aktuálních hrozbách a zavedených opatřeních v oblasti kybernetické bezpečnosti.
* Poskytuje útvarům zodpovědným za veřejné zakázky odbornou podporu a konzultace ohledně technických aspektů kybernetické bezpečnosti. Schvaluje konečnou verzi zadávací dokumentace z hlediska naplnění bezpečnostních standardů.
* Navrhuje změny strategie kybernetické bezpečnosti MMN a bezpečnostní politiky ISMS.

**Je oprávněn:**

* Stanovit závazné pokyny, metodiky či standardy v oblasti kybernetické bezpečnosti, které musí být v rámci organizace dodržovány (např. provozní pravidla, politiku řízení rizik apod.).
* V koordinaci s vedením organizace, stanovit jaká opatření budou realizována přednostně, a schvaluje koncepční změny či doplnění bezpečnostních plánů (např. změny plánu zvládání rizik).
* Stanovit minimální požadavky na úroveň poskytovaných služeb (např. v SLA) a sleduje jejich plnění.
* Stanovit přípravu a organizaci akceptačního řízení.
* Požadovat po dodavatelích či zhotovitelích doplnění potřebných bezpečnostních doložek do smluv a technologických postupů. Zajišťuje, aby smluvně převzaté závazky v oblasti kybernetické bezpečnosti byly v souladu s legislativou i interními předpisy.
* Stanovit rozsah a hranice ISMS s ohledem na aktiva a organizační bezpečnost, ve kterém stanoví, kterých organizačních částí a technických prvků se ISMS týká.
* Stanovit jednotnou metodiku pro identifikaci a hodnocení aktiv a metodiku pro stanovení kritérií pro přijatelnost rizik.
* Stanovit cíle kontinuity činností a strategii řízení kontinuity další činnosti pro oblast kybernetické bezpečnosti.
* Stanovit provozní pravidla a postupy ISMS.
* Stanovit plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání rizik včetně určení osoby zajišťující prosazování bezpečnostních opatření.
* Schvalovat závazné normy pro výběr, unifikaci a systemizaci technických a programových prostředků informačních technologií MMN.
* Metodicky řídit AKB.
* Schvalovat technické návrhy realizace kybernetické bezpečnosti vytvořené AKB.
* Vyžadovat od AKB technické řešení a detailní informace o realizovaných či navrhovaných opatřeních. Od ICT oddělení může vyžadovat nezbytné změny konfigurací, či nastavení systémů.
* Pokud jde o vysoká rizika nebo investice, iniciovat a vyžadovat od vedení organizace stanovisko k přijatelnosti rizik, uvolnění rozpočtových prostředků či organizační změny nutné k zabezpečení.
* Vyžaduje-li to situace (např. kvůli změně zákona či zjištěným nedostatkům), po příslušných interních útvarech vyžadovat úpravy zavedených směrnic, procesů a pravidel v souladu s platnou legislativou a aktuálními bezpečnostními předpisy, či trendy.
* Vyžadovat od odpovědných osob a dodavatelů pravidelné zprávy a podklady týkající se stavu kybernetického zabezpečení.
* Požadovat od garantů primárních aktiv zpracování a předložení:
	1. účelu systému a podmínek jeho provozování,
	2. identifikaci primárních aktiv a jejich rizik,
	3. stanovení bezpečnostních parametrů a úrovní systémem poskytovaných služeb SLA (Service Level Agreement).
* Požadovat od garantů podpůrných aktiv a administrátorů:
	1. identifikování podpůrných aktiv a jejich rizik,
	2. ohodnocení přijatelnosti těchto rizik včetně možnosti přenesení rizik,
	3. vyhodnocení účinnosti kybernetických bezpečnostních opatření.
* Vyžadovat okamžité nápravné opatření v případě zjištění závažných bezpečnostních nedostatků či incidentů.
1. **Objednávky**
2. Jednotlivé konzultařní činnosti budou sjednávány formou dílčích objednávek Objednatele zasílaných elektronicky na adresu uvedenou v této smlouvě
3. Objednávky budou obsahovat minimálně:
	* + odkaz na tuto Smlouvu;
		+ identifikační údaje smluvních stran;
		+ požadovaný předmět a rozsah dílčího plnění;
		+ požadovaný termín a místo (lokalita) dílčího plnění;
		+ místo předání dílčího plnění, je-li odlišné od sídla Objednatele;
		+ další specifické podmínky dílčího plnění, které nejsou stanoveny v této Smlouvě.
4. Zaslanou Objednávku Dodavatel potvrdí bez zbytečného odkladu, nejpozději do 3 pracovních dnů ode dne jejího doručení a potvrzenou objednávku zašle Objednateli elektronicky na adresu Objednatele uvedenou v této Smlouvě v č. VI., odst. 2.
5. **Cena a platební podmínky**
6. Cena provedených konzultačních činností za výkon role Manažera KB bude určena následovně. Bude-li to možné, tak pro ocenění konzultačních činností/služeb budou požity jednotkové ceny uvedené v této části Smlouvy, což jsou ceny stanovené Dodavatelem v jeho Nabídce. Jednotková cena konzultačních prací je stanovena na **XXXXXXXXX Kč** bez DPH za jednu hodinu práce.
7. Finanční limit této Rámcové dohody činí částku **1 990 000 Kč bez DPH**.
8. Dodavatel bere na vědomí a výslovně souhlasí s tím, že Objednatel neposkytuje zálohy.
9. Provedené práce budou hrazeny 1 x měsíčně na základě faktury Dodavatele, v níž budou uvedena čísla objednávek, na jejichž základě byly práce provedeny a každé dílčí (samostatné plnění) bude popsáno a oceněno v souladu s touto Dohodou.
10. Splatnost faktur je 30 kalendářních dnů od doručení faktury do sídla Objednatele.
11. Úhrada faktury bude provedena bezhotovostním převodem z účtu Objednatele na účet Dodavatele uvedený v záhlaví této Smlouvy.
12. **MÍSTO A LHŮTY PLNĚNÍ**
13. Místem plnění jsou pracoviště Objednatele v Jilemnici, Semilech a vzdálené přes videokonferenční hovory.
14. Obě strany se dohodly, že Objednatel v každé konkrétní objednávce stanoví požadovaný termín, respektive lhůtu provedení a požadovaný termín zahájení prací a Dodavatel na tuto lhůtu i termín přistoupí.
15. **PŘEDÁNÍ A PŘEVZETÍ, ODPOVÉDNOST**
16. Každá objednaná práce bude prokazatelně předána a převzata.
17. Za převzetí díla od MKB je odpovědný pracovník pracoviště strategií a rozvoje, XXXXXXXX XXXXXXX, e-mail XXXXXXXXXXX, mob. tel. XXXXXXXXXXXXX
18. MKB je odpovědný za soulad veškerých jím zpracovaných norem s příslušnými právními předpisy v oblasti kybernetické bezpečnosti.
19. **SMLUVNÍ POKUTY A ÚROK Z PRODLENÍ**
20. Pokud bude Dodavatel v prodlení s provedením prací proti sjednané lhůtě, respektive proti lhůtě uvedené v konkrétní objednávce Objednatele je povinen zaplatit Objednateli smluvní pokutu ve výši 200 Kč za každý i započatý den prodlení.
21. Pokud bude Objednatel v prodlení s úhradou faktury proti sjednanému termínu, je povinen zaplatit Dodavateli úrok z prodlení ve výši 0,1 % z dlužné částky za každý den prodlení.
22. **ODSTOUPENÍ OD SMLOUVY**
23. Od této smlouvy lze jednostranně odstoupit podle ustanovení § 1969 a § 2002–2005 občanského zákoníku.
24. **ZMĚNA RÁMCOVÉ DOHODY**
25. Změny této Rámcové dohody musí mít písemnou formu.
26. Jakákoliv ujednání či písemné záznamy se nestávají změnou rámcové dohody, pokud nejsou výslovně označena jako dodatek k Rámcové dohodě.
27. **DOBA TRVÁNÍ RÁMCOVÉ DOHODY**
28. Tato Smlouva se uzavírá na dobu určitou v trvání dvou let nebo vyčerpáním limitu
1 990 000 Kč bez DPH, podle toho, která skutečnost nastane dříve. Finanční limit nemusí být vyčerpán.
29. Zánikem Smlouvy nezanikají vzájemná práva a povinnosti smluvních stran z uskutečněných plnění, ze záruky za jakost, odpovědnosti za vady a sankce.
30. **ZÁVĚREČNÁ USTANOVENÍ**
31. Tato Smlouva byla vyhotovena ve dvou paré a řídí se právním řádem České republiky, zejména příslušnými ustanoveními občanského zákoníku a souvisejících právních norem a předpisů.
32. Tato Smlouva nabývá platnosti dnem jejího podpisu oprávněnými zástupci smluvních stran, uvedenými v čl. I. této smlouvy, účinnosti pak, s ohledem na ust. § 2 odst. 1 písm. m) zákona č. 340/2015 Sb., o registru smluv, uveřejněním v registru smluv, a to dle § 5 zákona o registru smluv, za současného respektování výjimek v zákoně o registru smluv uvedených. Uveřejnění smlouvy provede Objednatel v plném rozsahu s anonymizací nezbytných údajů.
33. Dodavatel výslovně uvádí, že tato smlouva neobsahuje žádné jeho obchodní tajemství, ani jiné informace, které by nemohly být uveřejněny či poskytnuty dle zákona č. 106/1999 Sb. či jiným způsobem.

**V Jilemnici dne V Praze dne**

Za Objednatele: Za Dodavatele:

………………………………………….. ……………………………………………….

MUDr. Jiří Kalenský

předseda představenstva

…………………………………………..

Ing. et. Ing. Imrich Kohút

člen představenstva