

## SMLOUVA O DÍLO

číslo smlouvy objednatele: SML/0672/2024

číslo smlouvy zhotovitele: 11/2024

*uzavřena v souladu ustanovením § 2586 a následujících zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „smlouva“) níže uvedeného dne mezi smluvními stranami, kterými jsou*

### Statutární město Přerov

zastoupené: [redacted] vedoucím Odboru vnitřní správy, na základě pověření dle části IV. Některé pravomoci vedoucích zaměstnanců dle článku 4 písm. a) Vnitřního předpisu č. 8/2018, ve znění pozdějších předpisů Organizačního řádu, kterým se vymezují kompetence Magistrátu města Přerova, ve znění pozdějších předpisů

se sídlem: Bratrská 709/34, Přerov I-Město, 750 02 Přerov  
IČ: 003 01 825  
DIČ: CZ00301825  
bankovní spojení: Česká spořitelna a.s.  
číslo transparentního účtu: [redacted]  
kontaktní osoba: [redacted] vedoucí Odboru vnitřní správy  
tel.: [redacted]  
e-mail: [redacted]

dále jen „**Objednatel**“

a

### I3 Consultants s.r.o.

vedená u Městského soudu v Praze, spisová značka C 126634  
zastoupená: [redacted], jednatelem  
se sídlem: Praha 6, Řepy, K Trnínám 945/34, 163 00  
IČ: 279 21 344  
DIČ: CZ27921344  
bankovní spojení: Komerční banka, a.s.  
č. účtu: [redacted]  
kontaktní osoba: [redacted] jednatel  
tel.: [redacted]  
e-mail: [redacted]  
Korespondenční adresa: Scheinerova1570/6, 628 00 Brno – Líšeň

dále jen „**Dodavatel**“

## ČLÁNEK 1

### PŘEDMĚT SMLOUVY

1. Předmětem této smlouvy je úprava práv a povinností smluvních stran v souvislosti s provedením hodnocení informačních rizik Statutárního města Přerov.
2. Dodavatel bere na vědomí, že obsah smlouvy včetně dodatků může být poskytnut žadateli v režimu zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a současně vyjadřuje souhlas s případným zveřejněním smlouvy včetně všech dodatků v registru smluv.
3. Dodavatel prohlašuje, že není nespolehlivým plátcem DPH a že v případě, že by se jím v průběhu trvání smluvního vztahu stal, tuto informaci neprodleně sdělí Objednateli.
4. Dodavatel prohlašuje, že je odborně způsobilý k zajištění předmětu této smlouvy.

## ČLÁNEK 2

### PŘEDMĚT PLNĚNÍ

1. Předmět plnění ze strany Dodavatele je podrobně uveden v nabídce, která tvoří přílohu č.2 a je nedílnou součástí této smlouvy.

## ČLÁNEK 3

### DOBA A MÍSTO PLNĚNÍ

1. Činnosti dle předmětu plnění budou zahájeny po podpisu smlouvy o dílo a dohodě s Objednatelem.
2. Doba plnění je stanovena od zahájení činností do 120 (slovy sto dvaceti) kalendářních dnů.
3. Místem plnění je Statutární město Přerov.

## ČLÁNEK 4

### CENA A PLATEBNÍ PODMÍNKY

#### 1. CENA DÍLA

- 1.1. Cena díla, uvedeného v Čl. 1 této smlouvy, je stanovena jako cena maximální, dohodnutá na základě nabídky ceny Dodavatele, a činí:

	Cena v Kč bez DPH	DPH 21 % v Kč	Cena v Kč včetně DPH
Provedení hodnocení informačních rizik v rozsahu 20 MD	165 000 Kč	34 650 Kč	199 650 Kč

- 1.2. Fakturovaná cena je celkovou částkou nejvýše přípustnou a obsahuje veškeré náklady Dodavatele, nutné a uznatelné k realizaci předmětu plnění dle této smlouvy.
- 1.3. Dojde-li v průběhu provádění díla ke změně výše příslušné sazby DPH či jiných poplatků stanovených příslušnými právními předpisy, bude účtována DPH k příslušným zdanitelným plněním či jiné poplatky ve výši stanovené novou právní úpravou.

## **2. ZPŮSOB PLATBY**

- 2.1. Platba bude poukázána pouze na základě faktury Dodavatele a po odsouhlasení a protokolárně převzatých výstupů ve formě akceptačního protokolu.

## **3. VYSTAVOVÁNÍ FAKTUR**

- 3.1. Celková odměna za plnění předmětu dle Čl. 2 této smlouvy bude Objednatelem placena na základě řádného daňového dokladu (faktury) za dodávku díla vystaveného Dodavatelem v souladu s dalšími podmínkami uvedenými v předchozím odstavci.
- 3.2. Faktura bude Dodavatelem vystavena v souladu s § 11 odst. 1 zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů a bude obsahovat náležitosti řádného daňového dokladu dle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.
- 3.3. Splatnost faktury bude 30 (slovy třicet) kalendářních dnů od jejího doručení Objednateli a po splnění podmínek uvedených v této smlouvě.
- 3.4. Objednatel je oprávněn vrátit fakturu před uplynutím lhůty její splatnosti bez zaplacení v případě, že neobsahuje zákonem stanovené a sjednané náležitosti anebo je vystavena na částku, která je v rozporu s touto smlouvou. Objednatel zároveň uvede důvod takového vrácení. V tomto případě běží nová lhůta splatnosti ode dne doručení opravené faktury Objednateli. Dodavatel v tomto případě nemá právo uplatňovat úrok z prodlení.
- 3.5. Strany se dohodly, že platba bude provedena na číslo účtu uvedené Dodavatelem v úvodu této smlouvy. Povinnost zaplatit je splněna dnem odepsání příslušné částky z účtu Objednatele.

## **ČLÁNEK 5**

### **PŘEDÁNÍ A PŘEVZETÍ DÍLA – AKCEPTACE**

1. Dodavatel se zavazuje v den ukončení díla předat Objednateli provedené dílo. V případě, že Objednatel odmítne dílo převzít, musí písemně uvést důvod.
2. Pokud Dodavatel připraví dílo k odevzdání před sjednaným termínem, zavazuje se Objednatel převzít toto dílo i v nabídnutém, oboustranně akceptovatelném, zkráceném termínu.

3. Dodavatel předá dílo v elektronické podobě, pokud nebude dohodnuto jinak.

## **ČLÁNEK 6**

### **GARANCE DODAVATELE**

1. Dodavatel prohlašuje, že je oprávněn k provádění činností dle předmětu této smlouvy v plném rozsahu, zejména, že je držitelem příslušných živnostenských oprávnění pokrývajících celý předmět plnění Dodavatele podle této smlouvy.
2. Dodavatel se zavazuje, že bude dodržovat a je schopen plnit právní a technické podmínky vyplývající ze závazných platných právních předpisů, vyhlášek a norem.
3. Dodavatel prohlašuje, že neumožňuje výkon nelegální práce ve smyslu zák. č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a ani neodebírání žádné plnění od osoby, která by výkon nelegální práce umožňovala. V případě, že se toto prohlášení ukáže v budoucnu nepravdivým a vznikne ručení Objednatele ve smyslu ust. § 141a a § 141b zák. č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů má Objednatel nárok na náhradu všeho, co za Dodavatele v souvislosti s tímto ručením plnil.

## **ČLÁNEK 7**

### **ODPOVĚDNOST ZA ŠKODU A SANKCE**

#### **1. ODPOVĚDNOST DODAVATELE**

- 1.1. Dodavatel odpovídá za to, že dílo ujednané touto smlouvou je vyhotoveno podle podmínek této smlouvy a že po trvání záruční doby bude mít vlastnosti dohodnuté v této smlouvě.
- 1.2. Dodavatel nezodpovídá za vady díla, které byly způsobeny použitím podkladů poskytnutých Objednavatelem a Dodavatel ani při vynaložení maximální péče, kterou po něm lze oprávněně požadovat, nemohl zjistit jejich nevhodnost, nebo na ně upozornil Objednavatele písemně a ten na jejich použití trval.
- 1.3. Záruční doba začíná plynout ode dne předání díla Objednavateli, tj. ode dne podpisu protokolu o předání a převzetí díla, a trvá 24 (slovy dvacet čtyři) měsíců. Záruka se vztahuje na dílo zpracované v souladu s platnou legislativou ke dni předání díla Objednateli.
- 1.4. Smluvní strany se dohodly, že v případě výskytu vady díla v záruční době, má Objednatel právo požadovat po Dodavateli bezplatné odstranění vady.
- 1.5. Dodavatel se zavazuje odstranit případnou vadu díla do 14 (slovy čtrnácti) kalendářních dní od oprávněné reklamace Objednavatele.

#### **2. SANKCE**

- 2.1. Bude-li Objednatel v prodlení s úhradou faktury, je Dodavatel oprávněn požadovat na Objednateli zaplacení úroku z prodlení ve výši 0,05 % z dlužné částky za každý započatý

den prodlení, a to až do doby zaplacení dlužné částky, a Objednatel je povinen takto požadovaný úrok z prodlení zaplatit.

- 2.2. Dodavatel se zavazuje, že v případě porušení důvěrnosti informací dle Čl. 8 této smlouvy zaplatí ten, kdo prokazatelně porušil tento závazek, druhé smluvní straně pokutu ve výši 50 000,- Kč (slovy padesát tisíc korun českých).

## **ČLÁNEK 8**

### **OCHRANA DŮVĚRNÝCH INFORMACÍ A OSOBNÍCH ÚDAJŮ**

1. Veškeré informace týkající se předmětu plnění dle této smlouvy, s nimiž bude Dodavatel přicházet v průběhu předjednání a v době po uzavření smlouvy do styku, jakož i výchozí podklady a materiály předané Objednatelem Dodavateli a výstupy a dokumenty, které Dodavatel získá v rámci své činnosti, jsou důvěrné. Tyto informace nesmějí být sděleny nikomu kromě Objednatele a třetích osob určených dohodou smluvních stran nebo třetím osobám v nezbytném rozsahu za účelem plnění povinností Dodavatele vyplývajících z této smlouvy a nesmějí být použity k jiným účelům než k plnění předmětu smlouvy.
2. Smluvní strany se zavazují, že během plnění Smlouvy i po jejím ukončení budou chránit důvěrné informace druhé strany tak, jako chrání svoje vlastní informace stejné důležitosti a zachovávat mlčenlivost o všech důvěrných informacích, o kterých se dozví od druhé smluvní strany v souvislosti s plněním Smlouvy. Objednatel považuje mimo jiné za důvěrné veškeré technické informace o jeho vnitřním prostředí a technické detaily týkající se technické infrastruktury, které nejsou obecně známé, a dále takové informace, které jím budou jako důvěrné výslovně označeny. Za porušení povinnosti mlčenlivosti se považuje i nezajištění vymazání dat z pevného disku a jejich zpřístupnění, byť nezaviněně, třetí osobě.
3. Výjimku z ochrany důvěrných informací tvoří ty informace, podklady a znalosti, které jsou všeobecně známé a dostupné. Dále pak informace obsažené v podkladech Objednatele nebo dokladech a stanoviscích získaných činností Dodavatele.
4. Poskytovatel je povinen zachovávat mlčenlivost o všech skutečnostech a informacích, které jsou obsažené v této Smlouvě a dále o všech skutečnostech a informacích, které mu byly v souvislosti s touto Smlouvou nebo jejím plněním jakkoliv zpřístupněny, předány či sděleny, nebo o nichž se jakkoliv dozvěděl, vyjma těch, které jsou v okamžiku, kdy se s nimi Poskytovatel seznámil, prokazatelně veřejně přístupné nebo těch, které se bez zavinění Poskytovatele veřejně přístupnými stanou (dále jen „důvěrné informace“). Poskytovatel nesmí důvěrné informace použít v rozporu s jejich účelem, nesmí je použít ve prospěch svůj nebo třetích osob a nesmí je použít ani v neprospěch Objednatele.
5. Poskytovatel se dále zavazuje zejména zajistit ochranu dat, které obsahují informace o osobních nebo citlivých údajích třetích osob, s nimiž přijde Poskytovatel (resp. jeho zaměstnanci) do kontaktu v rámci plnění této Smlouvy, a to v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů, a nařízením

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 a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), tzn. zejména zabezpečit, aby byla zachována mlčenlivost o těchto údajích, o všech bezpečnostních opatřeních, a aby zaměstnanci vyvíjeli snahu zabránit jakémukoliv zneužití těchto údajů jinou osobou. Povinnosti dle tohoto odstavce je Poskytovatel povinen zachovávat i po zániku závazku z této Smlouvy, vyjma případů, kdy se důvěrné informace stanou prokazatelně veřejně přístupné bez zavinění Poskytovatele. Povinnosti dle tohoto odstavce se nevztahují na případy, kdy je Poskytovatel povinen zveřejnit důvěrnou informaci na základě povinnosti uložené Poskytovateli platným právním předpisem nebo rozhodnutím orgánu veřejné moci.

## **ČLÁNEK 9**

### **ODSTOUPENÍ OD SMLOUVY**

1. Objednatel je oprávněn bez jakýchkoliv sankcí odstoupit od této Smlouvy v případě významné změny kontroly Dodavatele s tím, že změnou kontroly Dodavatele se rozumí změna ovládnutí Dodavatele, změna vlastnictví zásadních aktiv, popřípadě změna oprávnění nakládat s těmito aktivy, využívanými Dodavatelem k plnění Smlouvy.
2. Strany jsou oprávněny od Smlouvy odstoupit v případě závažného porušení smluvní nebo zákonné povinnosti druhou smluvní stranou. Odstoupení od Smlouvy nabývá účinnosti dnem doručení písemného oznámení o odstoupení druhé smluvní straně.
3. Tuto smlouvu lze též předčasně ukončit dohodou smluvních stran, jejíž součástí je i vypořádání vzájemných závazků a pohledávek.
4. Účinky každého odstoupení od Smlouvy nastávají okamžikem doručení písemného projevu vůle odstoupit od této Smlouvy druhé smluvní straně. Odstoupením od Smlouvy nezaniká nárok na náhradu škody vzniklé porušením Smlouvy ani oprávněného nároku na zaplacení smluvních pokut, resp. poskytnutí slev z cen.
5. Ukončením účinnosti této Smlouvy nejsou dotčena ustanovení Smlouvy o ochraně informací a ani další ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po zániku účinnosti této Smlouvy.

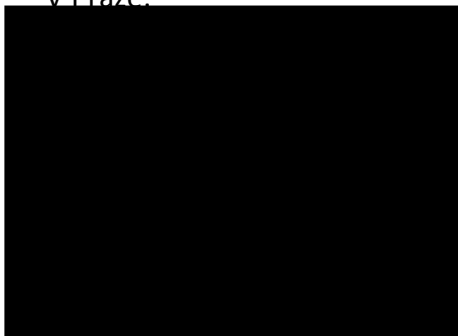
## **ČLÁNEK 10**

### **ZÁVĚREČNÁ USTANOVENÍ**

1. Právní vztahy vzniklé z této smlouvy, nebo s touto smlouvou související, se řídí zákonem č. 89/2012 Sb., občanským zákoníkem, ve znění pozdějších předpisů.
2. Dodavatel se zavazuje zajistit, že pro poskytování předmětu plnění dle Smlouvy budou využívány pouze aplikace a technologie, které jsou v souladu s platnou českou a evropskou legislativou, především s ohledem na licenční podmínky a předpisy upravující ochranu duševního vlastnictví.

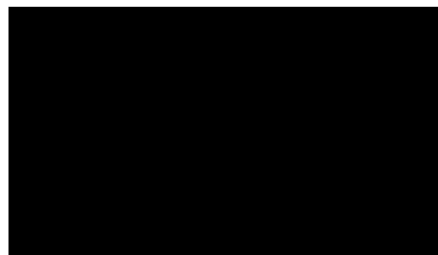
3. Tuto Smlouvu je možné měnit pouze písemnou dohodou smluvních stran ve formě vzestupně číslovaných dodatků k této Smlouvě, podepsaných za každou smluvní stranu osobou nebo osobami oprávněnými jednat jménem smluvních stran.
4. Spory vyplývající z této Smlouvy nebo vzniklé v souvislosti s ní nebo vzniklé v souvislosti s plněním mezi Objednatelem a Dodavatelem budou řešeny především dohodou. Pokud k dohodě nedojde, budou spory projednávány před soudy České republiky. V případě řešení sporů před soudem si smluvní strany sjednávají místní příslušnost prvoinstančního soudu podle místa sídla Objednatele.
5. Smluvní strany se dohodly, že objednatel uveřejní smlouvu prostřednictvím registru smluv ve smyslu zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů, bez zbytečného odkladu po podpisu smlouvy oběma smluvními stranami.
6. Tato Smlouva nabývá platnosti i dnem jejího podpisu oprávněnými osobami obou Smluvních stran a účinnosti dnem jejího uveřejnění prostřednictvím registru smluv ve smyslu zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů.
7. Tato Smlouva se vyhotovuje ve dvou stejnopisech s platností originálu, z nichž každá Smluvní strana obdrží po jednom vyhotovení.
8. Smluvní strany shodně prohlašují, že jsou si vědomy všech právních důsledků touto smlouvou vyvolaných, souhlasí se všemi jejími ustanoveními, s nimiž se podrobně seznámily, a na důkaz své svobodné a pravé vůle připojují vlastnoruční podpisy svých oprávněných zástupců.
9. Usnesením Rady města Přerova č. 515/20/4/2015 ze dne 11. června 2015 bylo schváleno nastavení výdajového účtu města číslo 27-1884482379/0800 jako účtu transparentního. Smluvní strany berou na vědomí a souhlasí s tím, že o platbách, které budou provedeny prostřednictvím tohoto účtu, budou veřejnosti dostupné informace na stránkách bankovního ústavu, v jaké výši, komu a za jakým účelem byly finanční prostředky z rozpočtu města uhrazeny.

V Praze:



Jednatel

V Přerově:



Vedoucí odboru vnitřní správy

**Příloha č. 1**  
**Realizační tým**

Jméno a příjmení	██████████
Pozice	Vedoucí realizačního týmu
E-mail	██████████
Telefon	██████████
Jméno a příjmení	██████████
Pozice	Specialista hodnocení informačních rizik
E-mail	██████████
Telefon	██████████
Jméno a příjmení	██████████
Pozice	Specialista hodnocení informačních rizik
E-mail	██████████
Telefon	██████████
Jméno a příjmení	██████████
Pozice	Specialista fyzické bezpečnosti
E-mail	██████████
Telefon	██████████
Jméno a příjmení	██████████
Pozice	Specialista architektury bezpečnosti
E-mail	██████████
Telefon	██████████



**Příloha č.2:**

**Nabídka „Provedení hodnocení informačních rizik Statutárního města Přerov“**

Dne 28. března 2024

ČN: 11/2024

**Statutární město Přerov**

Bratrská 709/34

Přerov I-Město, 750 02 Přerov

IČ: 00301825



**I3 Consultants**

INGENIOSUS INTER INGENIOSI

**NABÍDKA**

**“Provedení hodnocení informačních rizik Statutárního  
města Přerov“**

## 1. Souhrn nabídky

Společnost I3 Consultants s.r.o. si dovoluje předložit nabídku na provedení hodnocení informačních rizik u Statutárního města Přerov (dále také „SMP“). V předložené nabídce je popsáno naše pochopení Vašich potřeb a současně náš přístup k jejich zajištění.

Nabízíme pouze ty služby, které jsme schopni plně garantovat a jejich kvalitu prokázat odpovídajícími referencemi, které přesně odpovídají poptávanému a současně nabízenému řešení.

## 2. Návrh řešení

### 2.1. Prezentace metodiky identifikace a hodnocení aktiv a rizik

V rámci tohoto bodu bude provedeno představení metodiky pro identifikaci a hodnocení aktiv a rizik a nástroje pro výpočet rizik objednateli.

Metodika i nástroj budou objednateli předány k dalšímu využití.

### 2.2. Provedení identifikace primárních a podpůrných aktiv

Identifikace a hodnocení aktiv probíhá ve třech krocích:

1. Pohovory s vedoucími odborů/ oddělení k identifikaci a hodnocení primárních a podpůrných aktiv z hlediska požadavků na důvěrnost, integritu a dostupnost.
2. Pohovory s vedoucími pracovníky magistrátu k identifikaci kritičnosti (důležitosti) primárních aktiv.
3. Seskupení podpůrných aktiv stejných nebo obdobných vlastností do tzv. „typových aktiv“ a určení jejich vlastníků a provedení jejich hodnocení (hodnocení odpovídá nejvyšším hodnotám zařazeného podpůrného aktiva).

V rámci tohoto bodu bude v souladu s metodikou provedena:

- 1) Identifikace všech primárních aktiv (poskytovaných služeb a v nich zpracovávaných informací) realizovaných SMP a stanovení jejich garantů (vlastníků).
- 2) Identifikaci a hodnocení požadavků na důvěrnost, integritu a dostupnost realizovaných primárních aktiv (poskytovaných služeb) spadajících do regulované služby „Výkon svěřených pravomocí“.
- 3) Odůvodnění primárních aktiv, která nespádají do regulované služby.
- 4) Identifikaci a hodnocení podpůrných aktiv (technická aktiva, zaměstnanci, dodavatelé, objekty), prostřednictvím kterých se regulovaná služba zajišťuje.
- 5) Dekompozice aktiv na ICT infrastrukturu SMP (určení podpůrných technických aktiv infrastruktury ICT).
- 6) Sloučení obdobných podpůrných aktiv do tzv. „typových“ aktiv a určení jejich garantů.
- 7) Stanovení a popis vazeb mezi primárními a podpůrnými aktivy.

Výstupem z této etapy je:

- Identifikace a hodnocení aktiv v rozsahu
  - Katalog ohodnocených primárních aktiv SMP.
  - Katalog primárních aktiv regulované služby s uvedením jejich garantů.
  - Katalog primárních aktiv nespádajících do regulované služby s odůvodněním.
  - Katalog podpůrných aktiv.
  - Katalogu ohodnocených typových (seskupených podpůrných) aktiv s uvedením jejich garantů.
  - Popis vazeb mezi aktivy.
- V rámci přípravy katalogu podpůrných aktiv, kterými jsou realizována primární aktiva, dojde k seznámení dodavatele s ICT infrastrukturou SMP.

- Pokud by některé primární aktivum svým charakterem naplňovalo kritérium pro identifikaci regulované služby jiné, než je „Výkon svěřených pravomocí“, bude posouzeno, zda poskytovaná služba svým rozsahem spadá do režimu nižších či vyšších povinností.
- Pokud by tato alternativa nastala a identifikovaná služba by spadala do režimu vyšších povinností, pak by se stalo SMP poskytovatelem služby v režimu vyšších povinností a této skutečnosti by byly přizpůsobeny i další body nabídky, a to zejména v případě identifikace a konfrontace rozsahu přijatých bezpečnostních opatření, kde by se metrikou pro hodnocení stala vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností.

### 2.2.1. Provedení hodnocení informačních rizik

Hodnocení informačních rizik bude provedeno dle metodiky a nástrojem dodavatele.

Hodnocení hrozeb probíhá formou pohovorů s vlastníky typových aktiv, kterými jsou obvykle správci jednotlivých IS, aplikací, administrátoři a zaměstnanci, mající na starosti fyzickou bezpečnost objektů, personalista atd.

Hodnocení hrozeb a zranitelností, působících na typová aktiva, se provádí dle katalogu scénářů hrozeb a zranitelností uvedeného v návrhu Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby. Námí využívaný katalog je rozšířen o řadu specifických hrozeb a zranitelností.

Po hodnocení hrozeb následuje výpočet parciálních rizik a návrh vhodných opatření. Následně je prezentován stav hodnocení rizik po optimalizaci navržených opatření (po zohlednění navržených opatření). Následuje schválení tzv. akceptovatelných rizik vedením města. Po jejich akceptaci jsou stanovena jednotlivá bezpečnostní opatření a je vypočítána jejich účinnost. Výsledkem je stanovení priorit zavádění opatření, při kterém se zohledňuje efektivita daného opatření.

Výstupem z hodnocení rizik je:

- Hodnocení rizik
  - Hodnocení hrozeb a zranitelností
  - Výpočet rizika
  - Hodnocení rizika
  - Parciální rizika
  - Rozhodnutí o akceptaci rizik
  - Interpretace výsledků hodnocení rizik
- Zvládání rizik
  - Výběr opatření
  - Návrh prioritizace opatření dle účinnosti jednotlivých opatření

Dalšími výstupy z hodnocení rizik jsou:

- Návrh Prohlášení o aplikovatelnosti, které je přehledem identifikovaných bezpečnostních opatření, která jsou zavedena a návrh doporučených bezpečnostních opatření, která je nutné nebo vhodné zavést.
  - Pokud bude SMP identifikováno jako poskytovatel jediné regulované služby, kterou je služba „Výkon svěřených pravomocí“ bude základní metrikou pro hodnocení rozsahu bezpečnostních opatření návrh vyhlášky pro poskytovatele v režimu nižších povinností.
  - Pokud by v rámci bodu č. 1 nabídky došlo k identifikaci další poskytované regulované služby, která by spadala svým rozsahem do režimu vyšších povinností, bude základní metrikou pro hodnocení rozsahu bezpečnostních opatření návrh vyhlášky pro poskytovatele v režimu vyšších povinností.

- Návrh Plánu zvládnání rizik, který uvádí přehled bezpečnostních opatření, která jsou nutná pro odstranění nebo snížení kritických a důležitých rizik, identifikovaných:
  - na základě provedeného hodnocení informačních rizik
  - vyplývají z provedených pohovorů s vlastníky typových aktiv a stávající bezpečnostní architektury SMP

### 3. Nabídková cena

	Cena v Kč bez DPH	DPH 21 % v Kč	Cena v Kč včetně DPH
<b>Celková cena za provedení hodnocení informačních rizik v rozsahu 20 MD</b>	<b>165 000 Kč</b>	<b>34 650 Kč</b>	<b>199 650 Kč</b>

Nabídková cena je uvedena jako absolutní a nepřekročitelná částka za provedení celkové zakázky a obsahuje veškeré náklady se zakázkou spojené.

### 4. Doba plnění

Práce budou zahájeny od podpisu smlouvy a ukončeny do 120 dnů.

### 5. Prohlášení o mlčenlivosti

Společnost I3 Consultants s.r.o. se tímto, a následně prostřednictvím smlouvy o dílo zavazuje, že neprozradí žádné třetí straně informace týkající se objednatele nebo souvisejících organizací, které se její zaměstnanci budou mít možnost dozvědět v souvislosti s prováděním služeb pro objednatele.


Společnost se zavazuje obeznámit všechny své zaměstnance se závazky zde a následně ve smlouvě učiněnými, a že učiní vše, aby jeho zaměstnanci dostáli těmto závazkům.

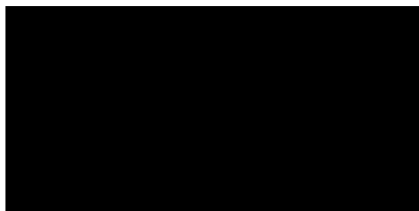
### 6. Závěr

Vážíme si skutečnosti, že jsme pro Vás mohli připravit tuto nabídku a věříme, že naše nabídka splňuje Vaše případné požadavky.

V případě nejasností či případných dalších požadavků nás prosím neváhejte kontaktovat.

Těšíme se na případnou spolupráci s Vámi.

  
 jednatel  
 I3 Consultants s.r.o.  
 Scheinerova 1570/6  
 628 00 Brno



 www.i3c.cz

## 7. Profil společnosti I3 Consultants s.r.o.

### Identifikační údaje

Obchodní název: I3 Consultants s.r.o.

Sídlo: K Trninám 945/34, 163 00 Praha 6 - Řepy

Adresa pobočky společnosti: Scheinerova 1570/6, 628 00 Brno



Datová schránka: maza9cz

Statutární orgán: [redacted] jednatel; [redacted] jednatel

IČ: 279 21 344

DIČ: CZ 279 21 344

Zapsáno v obchodním rejstříku vedeného Městským soudem v Praze oddíl C, vložka 126634

### Profil společnosti

I3 Consultants s.r.o. je ryze poradenskou společností, orientující se na poskytování služeb ve všech oblastech bezpečnosti informací, s důrazem na kybernetickou bezpečnost a ochranu osobních údajů.

Současně poskytujeme služby v oblasti zavádění systémů řízení a vzdělávání v oblasti bezpečnosti informací.

Společnost je držitelem certifikátu systému managementu kvality dle standardu ČSN EN ISO 9001:2009 a ČSN EN ISO/IEC 27001:2014.

Naši specialisté mají, jak v oblasti bezpečnosti informací, tak i v ochraně osobních údajů, více než patnáctiletou praxi a jsou držiteli následujících certifikátů:

- PRINCE 2 Practitioner
- Manažer kybernetické bezpečnosti
- Certifikovaný IT Security Manager
- Lead Auditor for Information Security Management Systems (ISO/IEC 27001:2013)
- Lead Auditor ČSN ISO/IEC 27001:2014
- Lead auditor ČSN ISO/IEC 20000
- OHSAS 18001:2007
- Auditor SM CSR (ČSN 01 0391)
- Lead auditor ČSN ISO/IEC 14001
- Lead auditor ČSN ISO/IEC 9001
- Pověřenec pro ochranu osobních údajů

### V oblasti bezpečnosti informací poskytujeme následující služby:

- Audity kybernetické bezpečnosti dle Vyhlášky č. 82/2018 Sb. (Vyhláška o kybernetické bezpečnosti)
- Audity bezpečnosti informací dle norem řady 27000 (ISMS)
- Analýzy rizik prováděných vlastním SW nástrojem
- Návrhy optimalizace bezpečnostních IT procesů
- Přípravu dokumentace k systému řízení bezpečnosti informací v rozsahu požadavků:
  - a. Zákona a vyhlášky o kybernetické bezpečnosti
  - b. Normy ČSN ISO/IEC 27001
- Pomoc při implementaci navrhovaných opatření
- Realizaci předcertifikačního auditu systému řízení bezpečnosti informací
- Doprovázení klienta při certifikačním auditu
- Zajištění výkonu role manažera a auditora kybernetické bezpečnosti u povinných osob, dle zákona o kybernetické bezpečnosti

### **V oblasti ochrany osobních údajů poskytujeme následující služby:**

- Audit ochrany osobních údajů
- Zavedení systému ochrany osobních údajů v rozsahu požadavků GDPR
- Provedení posouzení vlivu na ochranu osobních údajů (DPIA)
- Přípravu odborných stanovisek problematiky osobních údajů
- Poskytování konzultačních služeb:
  - a. podpora výkonu role pověřence pro ochranu osobních údajů,
  - b. řešení bezpečnostních událostí a incidentů,
  - c. řešení problematiky poskytování informací dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím,
  - d. zhodnocení a optimalizace odpovídajících opatření v rámci fyzické, personální a administrativní bezpečnosti.
- Zajištění výkonu role pověřence pro ochranu osobních údajů

### **V oblasti zavádění systémů řízení poskytujeme následující služby:**

- Přípravu na certifikaci norem ISO, spočívající ve zpracování dokumentace požadované standardy s minimálním zatížením zaměstnanců zákazníka. Nabízíme přípravu následujících standardů:
  - a. ISO 9001
  - b. ISO/IEC 27001
  - c. ISO/IEC 20000
  - d. ISO 14001
  - e. ISO 45001
- Podporu certifikovaných systémů řízení. Součástí námi poskytovaných služeb jsou zejména:
  - a. interní audity (příprava, realizace, zpracování výstupů),
  - b. návrhy na zlepšení systému řízení,
  - c. pomoc při zavádění a řízení opatření,
  - d. aktualizaci dokumentace,
  - e. aktualizace záznamů (politika, cíle a programy, přezkoumání vedením, plán školení atd.),
  - f. školení zaměstnanců,
  - g. příprava na audity prováděné certifikační organizací,
  - h. účast na dozorovém/recertifikačním auditu.

### **V oblasti vzdělávání nabízíme následující vzdělávací aktivity:**

- Vzdělávací kurzy pro manažery a auditory kybernetické bezpečnosti
- Základní školení bezpečnosti informací a kybernetické bezpečnosti pro zaměstnance
- Vzdělávací kurz pro pověřence pro ochranu osobních údajů
- Základní školení zpracování a ochrany osobních údajů pro zaměstnance
- E – learningové kurzy kybernetické bezpečnosti a zpracování a ochrany osobních údajů v členění:
  - a. Zaměstnanci
  - b. Správa ICT
  - c. Vedoucí zaměstnanci

### **Reference a garance kvality poskytovaných služeb**

#### **1 Vybrané referenční zakázky v oblasti energetiky**

GORDIC spol. s r.o.

- ✓ Poskytování služeb role manažera kybernetické bezpečnosti pro Vodovody a Pardubice – 2022-2023

ENERGETIKA TRINEC, a.s

- ✓ Konzultační činnost v oblasti KB při řešení GAP analýzy - 2022

UNIPETROL RPA, s.r.o.

- ✓ poskytování poradenských služeb v oblasti ochrany osobních údajů, obchodního tajemství a fyzické bezpečnosti – rámcová smlouva od r. 2020

Plzeňská teplárenská, a.s.

- ✓ Srovnávací analýza připravenosti společnosti Plzeňská teplárenská, a.s. pro plnění požadavků zákona o kybernetické bezpečnosti 181/2014 Sb. a souvisejících předpisů 2020–2021

Teplárna České Budějovice, a.s.

- ✓ konzultační činnosti spojené s funkcí a úkoly auditora kybernetické bezpečnosti dle vyhlášky č. 82/2018, o kybernetické bezpečnosti v platném znění- 2020–2023

Teplárna Písek a.s.

- ✓ Analýza stávajícího stavu zpracování a ochrany osobních údajů včetně posouzení připravenosti souladu s nařízením GDPR – 2018

Gas International s. r. o.

- ✓ Zpracování zásad ochrany osobních údajů a způsobů nakládání s nimi v rámci společnosti Gas International s. r. o. - 2016

## 2 Vybrané referenční zakázky v oblasti zdravotnictví

Nemocnice Havířov

- ✓ Vypracování bezpečnostní dokumentace a analýzy informačních rizik - 2022

Moravskoslezské datové centrum, příspěvková organizace

- ✓ Audit KB Slezské nemocnice Opava a rozdílové auditu KB nemocnic MSK - 2022

Slezská nemocnice Opava

- ✓ Audit, posouzení a analýza rizik v rámci připravenosti SNO na požadavky zákona a vyhlášky o kybernetické bezpečnosti – 2021
- ✓ Analýza procesů a zpracování dokumentace pro zajištění Business continuity planning v návaznosti na požadavky kybernetického zákona - 2022

Fakultní nemocnice Ostrava

- ✓ provedení GAP analýzy požadavků zákona o kybernetické bezpečnosti (ZKB) - 2017
- ✓ provedení GAP analýzy požadavků nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS) – 2017
- ✓ Studie IT bezpečnosti - 2011
- ✓ analýza současného stavu zpracování a ochrany osobních údajů, zpracování dokumentace pro ochranu osobních údajů - 2011
- ✓ vypracování strategie IT bezpečnosti - 2011

Nemocnice Vyškov

Proton Therapy Center Czech s.r.o.

Petra Clinic health s.r.o.

CMC – Centre Medical Care a.s.

Program Health Plus, s.r.o.

Bohemia – lázně a.s.

Slatinné lázně Třeboň s.r.o.

- ✓ zavedení systému ochrany osobních údajů dle GDPR – 2017–2019

Masarykův onkologický ústav

- ✓ Zavedení systému řízení bezpečnosti informací - 2011
- ✓ Zajištění služeb v oblasti bezpečnosti informačních systémů a ochrany osobních údajů – outsourcing výkonu role Manažera bezpečnosti IS a role Bezpečnostního správce IS – 2008–2012

Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace

- ✓ Konzultační, projektové a další služby v oblasti ochrany osobních údajů - 2013

MOJE AMBULANCE a.s.

- ✓ Poradenské služby v oblasti ochrany osobních údajů v souvislosti s povinnostmi vyplývajícími ze zákona č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů - 2012

Fakultní nemocnice Plzeň

- ✓ – vypracování Bezpečnostní politiky Fakultní nemocnice Plzeň - 2009
- ✓ - Posouzení a návrh standardu zabezpečení finanční hotovosti, depozitu a cenin - 2012
- ✓ - Zpracování dokumentace pro ochranu osobních údajů v kamerovém systému včetně podkladů pro registraci - 2012

### 3 Vybrané referenční zakázky v oblasti bezpečnosti informací, kybernetické bezpečnosti a implementace ISMS:

#### Státní fond životního prostředí České republiky

- ✓ Audit systému řízení kybernetické bezpečnosti – 2023

#### Dopravní podnik hl. města Prahy

- ✓ Audit kybernetické bezpečnosti - 2023

#### Úřad Národní rozpočtové rady

- ✓ Výkon role Manažera kybernetické bezpečnosti - 2023
- ✓ Implementace závěrů z auditu KB - 2022

#### VISITECH a.s.

- ✓ Řešení kybernetické bezpečnosti v nemocnicích MSK zadavatele Moravskoslezské datové centrum, p.o. – 2022 - dosud

#### Olomoucký kraj

- ✓ Poskytování služby Manažera kybernetické bezpečnosti – 2022-2023

#### Česká republika – Český úřad zeměměřický a katastrální

- ✓ Audity kybernetické bezpečnosti pro vybrané systémy zadavatele – 2022 - dosud

#### ANETE spol. s r.o.

- ✓ Vstupní analýza kybernetické bezpečnosti a vypracování řízené dokumentace kybernetické bezpečnosti - 2022

#### Česká republika Generální ředitelství cel

- ✓ Poskytnutí služeb interního auditu v oblasti kybernetické bezpečnosti pro systémy KB (KII a VIS) – 2022

#### Česká republika – Český báňský úřad

- ✓ Zajištění kybernetické bezpečnosti SBS - 2021-2023
- ✓ Analýza stavu kybernetické bezpečnosti a ustavení a zdokumentování systému řízení bezpečnosti informací u ČBÚ, výkon role manažera kybernetické bezpečnosti

#### Česká republika – Kancelář Poslanecké sněmovny

- ✓ Provedení auditu kybernetické bezpečnosti v souladu s vyhláškou č. 82/2018 Sb. - 2021

#### Ministerstvo pro místní rozvoj ČR

- ✓ zajištění bezpečnostního dohledu MS 2014+ v oblasti řízení bezpečnosti informací a oblasti zpracování a ochrany osobních údajů - 2015–2021
- ✓ Úprava a vytvoření dokumentace systému NEN podle vyhlášky č. 82/2018 Sb. (vyhláška o kybernetické bezpečnosti) - 2019
- ✓ GAP analýza kybernetické bezpečnosti – 2015

#### Ministerstvo práce a sociálních věcí - 2015

- ✓ Komplexní analýza oblasti řízení bezpečnosti a následná implementace jednotného systému řízení bezpečnosti v rezortu MPSV a ostatních organizačních složek a příspěvkových organizací rezortu (v souladu s požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti)  
Následně zavedení procesů jednotného systému řízení bezpečnosti v resortu MPSV, zajištění efektivního řízení následujících oblastí bezpečnosti: fyzická bezpečnost; kybernetická a informační bezpečnost; ochrana osobních údajů; personální bezpečnost; administrativní bezpečnost. Revize a schválení finálních výstupů. Prezentace finálních výstupů projektu zadavateli. Počet uživatelů IS: 23 000

#### Ministerstvo vnitra – Policejní prezidium České republiky – KB

- ✓ Aktualizace současné Bezpečnostní politiky odboru informatiky a provozu informačních technologií Policejního prezidia České republiky – 2016

#### Ministerstvo životního prostředí ČR



- ✓ Zpracování Vrcholové bezpečnostní politiky Ministerstva životního prostředí ČR a zavedení procesního modulu řízení bezpečnosti u MŽP v rozsahu standardu ČSN ISO/IEC 27001, realizace interních auditů, poskytování poradenství v oblasti OUI a OOÚ – 2010, 2012, 2015
- Generální finanční ředitelství
- ✓ ustavení systému řízení bezpečnosti informací - 2014
- Český statistický úřad
- ✓ srovnávací analýza souladu systémů s požadavky zákona o kybernetické bezpečnosti – 2015
- Česká školní inspekce
- ✓ Validace akceptace, ISVS certifikace a implementace pravidel kybernetické bezpečnosti pro informační systém projektu NIQES - 2015
- Česká republika – Úřad pro civilní letectví
- ✓ Vypracování odborné studie, ve které dodavatel posoudí připravenost ÚCL na vybrané aspekty zákona č.181/2014 Sb., o kybernetické bezpečnosti včetně Vyhlášky č.316/2014 Sb., ZKB a Vyhlášky č.317/2014 Sb., o významných informačních systémech a jejich určujících kritériích - 2015
- Moravskoslezský kraj
- ✓ Vytvoření „Bezpečnostní politiky ICT pro příspěvkové organizace Moravskoslezského kraje - 2020
- Zlínský kraj – Krajský úřad Zlínského kraje
- ✓ ustavení systému řízení bezpečnosti informací – 2017–2018
- Liberecký kraj
- ✓ ustavení systému řízení bezpečnosti informací – 2017
- Pardubický kraj
- ✓ úprava metodiky analýzy rizik Krajského úřadu Pardubického kraje - 2018
- Statutární město Brno – Magistrát města Brna, Městská policie Brno
- ✓ ustavení systému řízení bezpečnosti informací - 2011
  - ✓ outsourcing výkonu role Manažera bezpečnosti informací – 2012 - dosud
- Statutární město Olomouc – Magistrát města Olomouc
- ✓ ustavení systému řízení bezpečnosti informací v rozsahu norem ISO 27000 a zákona o kybernetické bezpečnosti 2016–2017
- České dráhy, a.s.
- ✓ Analýza rizik vybraných informačních systémů ČD (potencionální IS ZS dle z. 181/2014 Sb., o kybernetické bezpečnosti) pro České dráhy, a. s.: Vstupní analýza jednotlivých IS, Analýza rizik IS, Plán zvládnání rizik a návrh konkrétních opatření - 2021
  - ✓ vypracování analýzy IT rizik s ohledem na ZKB - 2017
- Unicontrols a.s.
- ✓ ustavení systému řízení bezpečnosti informací - 2017
- Panasonic AVC Networks Czech, s.r.o.
- ✓ poradenská činnost, interní audity, analýzy rizik, aktualizace dokumentace – 2016 - dosud
  - ✓ analýza rizik – 2015
  - ✓ ustavení systému řízení bezpečnosti informací – 2012
- ČD-Telematika a.s.
- ✓ ustavení systému řízení bezpečnosti informací – 2010, aktualizace ISMS – 2015
- UNIS, a.s. – 2009, 2012, 2015, 2018
- ✓ Příprava k certifikaci ISO 27001 (ISMS)
  - ✓ Příprava k certifikaci ISO 20000 (ITSM)
- Dopravní podnik města Brna, a.s.
- ✓ ustavení systému řízení bezpečnosti informací – 2015
- Brněnské komunikace a.s.
- ✓ ustavení systému řízení bezpečnosti informací – 2012
  - ✓ Zabezpečení činností v oblasti bezpečnosti informací – 2012 – dosud
- SWIETELSKY stavební s.r.o.
- ✓ ustavení systému řízení bezpečnosti informací - 2019
- CD Cargo, a.s.
- ✓ Provedení interního auditu ISMS – 2017, 2018, 2019
- Povodí Moravy, s.p.

- ✓ Interní audit ISMS – 2018
- Zaměstnanecká pojišťovna Škoda
- ✓ Interní audit ISMS - 2020

#### **4 Vybrané referenční zakázky v oblasti ochrany osobních údajů**

##### **4.1 Zavedení systému ochrany osobních údajů dle GDPR v rozsahu**

- ✓ vstupní analýza požadavků GDPR
- ✓ analýza rizik GDPR
- ✓ vypracování interních předpisů a potřebné související řídicí dokumentace
- ✓ školení GDPR

##### pro státní správu a samosprávu:

- ✓ Ministerstvo průmyslu a obchodu
- ✓ Zlínský kraj
- ✓ Jihočeský kraj
- ✓ Jihomoravský kraj
- ✓ Olomoucký kraj
- ✓ Liberecký kraj
- ✓ Pardubický kraj
- ✓ Ústecký kraj

##### pro společnosti:

- ✓ Panasonic AVC Networks Czech, s.r.o.
- ✓ ŠKODA JS a.s.
- ✓ SITEL, spol. s r.o.
- ✓ CENTRA a.s.
- ✓ X-TRADE BROKERS DOM MAKLERSKI SPÓŁKA AKCYJNA, organizační složka
- ✓ STAREZ – SPORT, a.s.
- ✓ Vojenské lesy a statky ČR, a.s.
- ✓ Brněnské komunikace, a.s.

pro města a obce (Města Jaroměř, Kroměříž, Chropyně, Jeseník, Rožnov pod Radhoštěm, Ruda nad Moravou, Mikulov, Oslavany, Šternberk, Valašské Meziříčí, Uherské Hradiště, Uničov, Mikroregion Kahan)

pro školy, školská a sociální zařízení (více než 400)

##### **4.2 Výkon funkce pověřence GDPR**

- ✓ Statutární město Brno, Městská policie Brno
- ✓ Centrum pro regionální rozvoj České republiky
- ✓ Město Oslavany
- ✓ Město Chropyně
- ✓ obce Mikroregionu Kahan
- ✓ Více než 250 škol (MŠ, ZŠ, SŠ) a školských zařízení (DDM, SVČ, PPP)
- ✓ cca 200 příspěvkových organizací Moravskoslezského kraje
- ✓ Střediska sociální péče

##### **4.3 Poskytování trvalé podpory rutinního provozu GDPR (podpory pověřence pro OOU)**

- ✓ Zlínský kraj
- ✓ Statutární město Kladno
- ✓ Statutární město Olomouc
- ✓ Města Rožnov pod Radhoštěm, Mikulov, Jeseník, Uničov
- ✓ Brněnské komunikace a.s.

## **5 Vybrané referenční projekty (provedení certifikačního auditu ISMS) realizované našimi auditory**

### **5.1 pro LRQA**

- ✓ NESS Czech s.r.o.
- ✓ INFAS, a.s.
- ✓ Městská policie Brno
- ✓ AERO Vodochody, a.s.
- ✓ Národní agentura pro komunikační a informační technologie s. p.
- ✓ EMM, spol. s.r.o
- ✓ gsnet.cz s.r.o
- ✓ Unis a.s.
- ✓ Výzkumný ústav jaderné energetiky
- ✓ TECHNISERV IT, spol. s r.o.
- ✓ Česká pošta, s.p.

### **5.2 pro CERT-ACO, s.r.o.**

- ✓ VUSTE – APIS s.r.o.
- ✓ Šroubárny Trutnov
- ✓ Krajský úřad Moravskoslezského kraje
- ✓ Armatury a potrubní díly
- ✓ Colsys

### **5.3 pro United Registrar of Systems (Holdings) Ltd.**

- ✓ Microsys Brno
- ✓ AKR1
- ✓ ARION
- ✓ Avservis (Awigo)
- ✓ Forcorp\_group
- ✓ Henig
- ✓ Changhong Europe Electric
- ✓ Multima
- ✓ Valdman