Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Smlouva o dílo č. objednatele 20/09740/22
„SRUB – Strategický rozvoj Uherského Brodu 2022+ KA 1:
Řízení kvality – zavedení systému ISO/IMC
uzavřená dle ustanovení § 2586 a násl. zákona č. 89/2012 Sb.,
občanský zákoník, ve znění pozdějších předpisů

Město Uherský Brod
se sídlem: Masarykovo nám. 100, 688 01 Uherský Brod
IČO: 002 91 463
DIČ: CZ00291463
Zastoupené: Ing. Ferdinandem Kubáníkem, starostou
Bankovní spojení:

Osoba oprávněná jednat ve věcech technických:

Ing. Kamil Válek, tajemník *(dále jen „objednatel")*

a

DoxoLogic, s.r.o.
se sídlem: **Karolinská 661/4, 186 00 Praha 8**
zastoupena: Bc. Martinem Listopadem, jednatelem
IČO: 279 03 656
DIČ: CZ27903656
bankovní spojení: Unicredit Bank
číslo účtu: 2112895098/2700
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 125420

(dále jen „zhotovitel")

uzavírají níže uvedeného dne, měsíce a roku

tuto smlouvu o dílo:

I. Předmět smlouvy

1. Zhotovitel se na základě smlouvy zavazuje na svůj náklad a nebezpečí provést pro objednatele dílo „SRUB - Strategický rozvoj Uherského Brodu 2022+ KA 1: Řízení kvality – zavedení systému ISO/IMC, Dílčí plnění 1 – Zavedení systému ISO/IEC 27000 (ISMS), Dílčí plnění 2 – Certifikace systému ISO/IEC 27000 (ISMS)" registrační číslo projektu CZ.03.4.74/0.0/0.0/17_080/0010103 (dále jen „dílo"), a objednatel se zavazuje řádně provedené dílo převzít a zaplatit zhotoviteli cenu za jeho provedení.

2. Podkladem po uzavření smlouvy je nabídka zhotovitele ze dne 17.11.2021, která byla vypracována na základě výzvy objednatele k podání nabídky v zadávacím řízení na veřejnou zakázku na služby. SRUB - Strategický rozvoj Uherského Brodu 2022+ KA 1: Řízení kvality – zavedení systému ISO/IMC, Dílčí plnění 1 – Zavedení systému ISO/IEC 27000 (ISMS), Dílčí plnění 2 – Certifikace systému ISO/IEC 27000 (ISMS)".

II. Specifikace díla

1. Zhotovitel zajistí provedení díla v rozsahu a struktuře specifikované v příloze č. 1 smlouvy, která je nedílnou součástí smlouvy. Součástí díla jsou veškeré práce a služby nezbytné pro řádné a úplné zhotovení díla.
2. Dílo bude dodáno do sídla objednatele ve formě a počtu vyhotovení dle specifikace uvedené v příloze č. 1 smlouvy.
3. Zhotovitel prohlašuje, že se s rozsahem díla seznámil, že je schopen dílo ve smluvené lhůtě dodat a že veškeré náklady spojené se zhotovením díla jsou zahrnuty v ceně díla. Zhotovitel se zavazuje dílo provést s potřebnou péčí, v ujednaném čase a obstarat vše co je k provedení díla potřeba, v souladu s podklady pro provedení díla. Zhotovitel prohlašuje, že se před uzavřením smlouvy seznámil se všemi podklady nezbytnými pro provedení díla. Zhotovitel bere na vědomí, že nezbytná součinnost objednatele k provedení díla spočívá v umožnění přístupu zhotoviteli k těmto podkladům a ve výkonu oprávnění objednatele udílet zhotoviteli písemné závazné pokyny při provádění díla. Bude-li zhotovitelem požadována po objednateli jakákoliv součinnost s prováděním díla, je povinen ji před započetím jakéhokoliv plnění ze smlouvy dostatečně a prokazatelně písemně specifikovat. Objednatel se zavazuje poskytnout zhotoviteli nezbytné podklady vztahující se k předmětu smlouvy, které má ve svém držení a které si specifikuje zhotovitel.
4. Finální podoba díla podléhá předchozímu schválení ze strany objednatele.
5. Zhotovitel tohoto dílčího plnění se zavazuje k poskytnutí plné součinnosti při procesu certikace tak, aby vzájemná komunikace mezi Zhotovitelem Dílčího plnění 1 Zhotovotelem Dílčího plnění 2 probíhala napřímo bez účasti Objednatele. Jedná se zejména o předání pokladů, komunikaci při procesu certifikace jakož i veškerou nezbytnou součitnnost, která s procesem certifikace souvisí. Tuto součinnost se Zhotovitel zavazuje poskytovat až do úspěšného dokončení certifikačního procesu.
6. Objednatel si dle § 105 zákona 134/2016 Sb. o zadávání veřejných zakázek vyhrazuje požadavek, že určitá část plnění díla nesmí být plněna poddodavatelem. Objednatel stanoví podmínku, že nesmí být poddodavatelsky zajištěn:
   - výkon funkce vedoucího realizačního týmu.

III. Čas a místo plnění

1. Zhotovitel zajistí předání a převzetí díla v kvalitě a množství dle čl. II. smlouvy do sídla objednatele **do 30.6.2022,** není-li dále uvedeno jinak. Dílo je provedeno, je-li dokončeno a předáno. Zahájení plnění veřejné zakázky: dnem účinnosti smlouvy o dílo.

2. Milníky stanovené objednatelem:

Dílčí plnění 1:

Fáze	**Etapa**	**Termín (T = termín uzavření smlouvy)**
Analytická část	1. Rozdílová analýza	T + 10 kalendářních dní
Analytická část	2. Stanovení rozsahu systému	T + 15 kalendářních dní
Analytická část	3. Definice Politiky ISMS, cílů a odpovědností	T + 30 kalendářních dní
Analytická část	4. Analýza rizik	T + 50 kalendářních dní
Návrhová část	5. Bezpečnostní standardy, bezpečnostní dokumentace	T + 80 kalendářních dní
Návrhová část	6. Doporučení k aktualizaci a údržbě bezpečnostních politik a dokumentace	T + 80 kalendářních dní
Realizační část	7. Implementace ISMS	T + 110 kalendářních dní
Realizační část	8. Ověření připravenosti k certifikačnímu auditu	T + 120 kalendářních dní
Realizační část	9. Součinnost při certifikačním procesu	T + 150 kalendářních dní

Dílčí plnění 2:

Fáze	**Etapa**	**Termín (T = termín uzavření smlouvy)**
Realizační část	10. Zajištění certifikačního auditu	T + 120 kalendářních dní
Realizační část	11. Certifikace dle normy ČSN ISO/IEC 27000	**T + 150 kalendářních dní**

3. Objednatel si vyhrazuje v souladu s § 100 odstavec 1 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, změnu závazku, a to možnost protokolární předání a převzetí díla o tolik dnů později, o kolik bude později účinnost této smlouvy oproti předpokladu(tj. do 30.1.2022).

4. O předání a převzetí díla bude vyhotoven předávací protokol podepsaný příslušným zástupcem objednatele a zástupcem zhotovitele. Dílo lze předat pouze v pracovních dnech

od 8 hod. do 14 hod. Zhotovitel je povinen oznámit objednateli termín předání díla 3 pracovní dny předem písemně poštou, e-mailem či jiným prokazatelným způsobem. Smluvní strany se dohodly, že objednatel není povinen dílo převzít, pokud toto dílo vykazuje i jen drobné vady či nedodělky.

5. Nebezpečí škody na díle a vlastnické právo k dílu přechází na objednatele dnem protokolárního předání a převzetí díla.
6. Místo předání díla je místo sídla objednatele, tj. Masarykovo nám. 100, 688 01 Uherský Brod (vyjma míst v Uherském Brodě pro veřejné projednávání).

IV. Cena díla

1. Cena za provedení díla v rozsahu čl. I. a II. této smlouvy je stranami dohodnuta ve výši:

   Cena za dílo bez DPH: **386.720,00** Kč

   DPH 21 %: **81.211,20** Kč

   Celková cena díla včetně DPH: 467.931,20 Kč

2. Celková cena díla zahrnuje veškeré náklady a zisk zhotovitele nezbytné k řádnému a včasnému provedení díla. Zhotovitel prohlašuje, že se předem seznámil se všemi okolnostmi a podmínkami, které by mohly mít jakýkoliv vliv na stanovení ceny díla. Celková cena díla obsahuje veškeré náklady zhotovitele nezbytné k realizaci díla. Tato cena obsahuje předpokládané zvýšení ceny v závislosti na čase plnění, předpokládaný vývoj cen vstupních nákladů.
3. Cenu je možné změnit jen v případě, že v průběhu provádění díla dojde ke změnám sazeb DPH.
4. V případě změny sazby daně z přidané hodnoty nejsou smluvní strany povinny uzavírat ke smlouvě dodatek. Platná sazba daně z přidané hodnoty bude k datu uskutečnění zdanitelného plnění uvedena v daňovém dokladu – faktuře.
5. Není-li zhotovitel v době uzavření smlouvy plátcem DPH a v průběhu realizace smlouvy se plátcem DPH stane, nesmí důsledky této změny jít k tíži objednatele a za tím účelem poskytne zhotovitel objednateli slevu v takové výši, aby fakturovaná cena s DPH byla nejvýše rovna výši ceny dle této smlouvy sjednané za totéž plnění v době, kdy zhotovitel plátcem DPH nebyl.

V. Platební podmínky

1. Cena za provedení díla bude fakturována následovně: zhotovitel vystaví fakturu – daňový doklad ihned po protokolárním předání a převzetí díla dle čl. III. odst. 1, nejpozději však do 15 dnů od protokolárního předání a převzetí díla. Součástí faktury bude předávací protokol.
2. Splatnost faktury se sjednává na 30 dnů od jejího doručení objednateli; dnem připsání je den odepsání finančních prostředků z účtu objednatele.
3. Faktura musí obsahovat všechny náležitosti stanovené obecně závaznými právními předpisy, v případě faktur – daňových dokladů náležitosti dle zákona o DPH, zejména:

a) označení faktury a její číslo;

b) označení objednatele – název, sídlo, IČ a DIČ, bankovní spojení;

c) označení zhotovitele – obchodní firma, sídlo, IČ a DIČ, bankovní spojení;

d) název díla, číslo smlouvy objednatele a den jejího uzavření;

e) předmět díla;

f) cena – fakturovaná částka;

g) DPH v platné výši;

h) datum vystavení a odeslání faktury;

i) datum uskutečnění zdanitelného plnění;

j) splatnost faktury;

k) razítko a podpis oprávněné osoby, stvrzující oprávněnost, formální a věcnou správnost faktury,

l) přílohou faktury k úhradě díla bude předávací protokol dle čl. III. smlouvy.

4. Na faktuře musí být rovněž uvedena informace povinné publicity: „Výdaj je spolufinancován Evropským sociálním fondem prostřednictvím Operačního programu Zaměstnanost. Projekt „SRUB – Strategický rozvoj Uherského Brodu 2022+" registrační číslo CZ.03.4.74/0.0/0.0/17_080/0010103.

5. V případě, že faktura nebude vystavena oprávněně, bude obsahovat nesprávné údaje nebo nebude obsahovat náležitosti v souladu se smlouvou, je objednatel oprávněn vrátit ji zhotoviteli. V takovém případě se přeruší plynutí lhůty splatnosti a nová lhůta splatnosti začne plynout vždy až dnem doručení opravené nebo oprávněně vystavené faktury objednateli.

6. Zhotovitel se zavazuje použít na faktuře bankovní účet zveřejněný v aplikaci „Registr plátců DPH" podle § 96 zákona o DPH.

7. Objednatel si vyhrazuje právo uplatnit institut zvláštního způsobu zajištění daně dle § 109a zákona o DPH a hodnotu plnění odpovídající dani z přidané hodnoty uhradit v termínu splatnosti příslušné faktury stanoveném dle smlouvy přímo na osobní depozitní účet zhotovitele vedený u místně příslušného správce daně v případě, že:

   a) zhotovitel bude ke dni uskutečnění zdanitelného plnění zveřejněn v aplikaci „Registr plátců DPH" jako nespolehlivý plátce, nebo

   b) zhotovitel bude ke dni uskutečnění zdanitelného plnění v insolvenčním řízení, nebo

   c) bankovní účet zhotovitele určený k úhradě plnění uvedený na faktuře nebude správcem daně zveřejněn v aplikaci „Registr plátců DPH".

   Objednatel nenese odpovědnost za případné penále a jiné postihy vyměřené či stanovené správcem daně zhotoviteli v souvislosti s potenciálně pozdní úhradou DPH, tj. po datu splatnosti této daně. Nastanou-li okolnosti, umožňující objednateli uplatnit zvláštní způsob zajištění daně, bude objednatel o této skutečnosti zhotovitele informovat.

   Uplatní-li objednatel institut zvláštního způsobu zajištění daně ve shodě s tímto ujednáním a uhradí příslušnou částku na účet zhotovitele vedený u jeho místně

příslušného správce daně, bude tato úhrada považována za splnění části závazku objednatele odpovídající příslušné výši DPH sjednané jako součást smluvní ceny za zdanitelné plnění.

VI. Sankce

1. V případě prodlení zhotovitele s předáním díla v termínu dle čl. III. smlouvy je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 0,5 % z celkové ceny díla s DPH za každý den prodlení.
2. V případě prodlení objednatele se zaplacením ceny díla je zhotovitel oprávněn požadovat zaplacení úroku z prodlení v souladu s platnými a účinnými právními předpisy.
3. V případě převzetí díla objednatelem a prodlení zhotovitele s odstraněním vad a nedodělků díla zjištěných při předání a převzetí díla, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 0,5 % z celkové ceny díla s DPH za každou vadu a nedodělek a každý den prodlení.
4. V případě prodlení s odstraněním vad díla zjištěných po předání a převzetí díla je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 0,1 % z celkové ceny díla s DPH za každou vadu a každý den prodlení.
5. Zhotovitel je povinen uhradit objednateli smluvní pokutu ve výši 10.000 Kč za každý jednotlivý případ, pokud změní konkrétní osobu tvořící projektový tým bez předchozího písemného souhlasu objednatele nebo pokud nový člen týmu nebude splňovat požadované kvalifikace uvedené v zadávacích podmínkách.
6. Zhotovitel je povinen uhradit objednateli smluvní pokutu ve výši 5.000 Kč, pokud poruší závazek mlčenlivosti sjednaný ve smlouvě.
7. V případě nedodržení povinnosti zhotovitele, která vyplývá z řádného plnění smlouvy a předmětu (např. nespolupracování s externím metodikem) a není uvedena v odst. 1, 3 až 6 tohoto článku smlouvy, se sjednává smluvní pokuta ve výši 1.000 Kč za každé takové porušení (např. nedodržení povinnosti dle čl. V. odst. 5 smlouvy apod.). Je-li stanovena doba plnění takové povinnosti, jedná se o smluvní pokutu za každý i započatý den prodlení s jejím splněním.
8. Zhotovitel bere na vědomí svou povinnost dokončit a předat dílo řádně a ve sjednaném termínu (s výhradou změny termínu). Zhotovitel prohlašuje, že si je plně vědom hodnoty a významu dodržení tohoto termínu pro vznik nároku objednatele na dotaci z projektu SRUB – Strategický rozvoj Uherského Brodu 2022+ z Operačního programu Zaměstnanost a své odpovědnosti za případné porušení této povinnosti. Pro případ, že zhotovitel poruší svou povinnost dílo včas dokončit a předat objednateli, a objednateli z tohoto důvodu nevznikne nárok na dotaci, je zhotovitel povinen zaplatit objednateli smluvní pokutu až do výše nepřiznané dotace za příslušnou část projektu (KA1 1 část PRM). Uplatněním smluvních pokut dle smlouvy není dotčen nárok na náhradu škody v plném rozsahu. Zhotovitel bere na vědomí, že jeho vadné plnění může mít za následek vznik škody na straně objednatele spočívající v krácení nebo nepřiznání dotace.
9. Smluvní pokuta je splatná do 21 dnů ode dne, kdy objednatel vyzval zhotovitele k její úhradě.
10. Za podstatné porušení smlouvy je považováno mj. prodlení zhotovitele s předáním díla o více než 14 dní. Při takovém porušení je objednatel oprávněn odstoupit od smlouvy

písemným prohlášením doručeným zhotoviteli. Odstoupením od smlouvy není dotčen případný nárok objednatele na náhradu škody a smluvní pokutu.

11. Objednatel je oprávněn během realizace smlouvy nebo i po jejím ukončení jednostranně započítat svou pohledávku vůči zhotoviteli proti pohledávce zhotovitele za objednatelem plynoucí ze smlouvy.

VII. Jiná ujednání

1. Zhotovitel poskytuje objednateli k užití díla licenci podle § 2371 občanského zákoníku. Tato licence je udělena ke všem způsobům užití díla dle § 12 odst. 4 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, a to v rozsahu územně a množstevně neomezeném na dobu trvání autorskoprávní ochrany díla. Objednatel smí dílo nebo jeho název upravit či jinak měnit. Objednatel je oprávněn poskytnout oprávnění tvořící součást licence třetím osobám zcela nebo zčásti (podlicence). Objednatel není povinen licenci využít. Smluvní strany se dohodly, že odměna za poskytnutou licenci je součástí ceny dle čl. IV. odst. 1 smlouvy.

2. Na žádost objednatele budou dle jeho volby realizovány schůzky v souladu s termíny uvedenými v příloze č. 1. objednatele a zhotovitele za účelem kontroly způsobu provádění díla. Schůzky dle popisu z Výzvy k podání nabídky budou realizovány v sídle objednatele, pokud nepříznivá epidemická situace nepřevede jednání do elektronického prostředí se vzdáleným přístupem. Objednatel požádá zhotovitele o schůzku alespoň dva pracovní dny před stanoveným termínem schůzky. Účast na jednání je povinen zhotovitel nejpozději den předem potvrdit a v případě omluvy dohodnout se na náhradním termínu. Zhotovitel je povinen řídit se při provádění díla pokyny objednatele. Zhotovitel je povinen písemně poštou nebo e-mailem upozornit objednatele na případnou nevhodnost jeho pokynů.

3. Zhotovitel poskytuje objednateli záruku za jakost díla. Záruční doba počíná běžet dnem protokolárního předání a převzetí díla objednatelem a trvá 24 měsíců. Zhotovitel odpovídá za vady, které má dílo v době jeho předání objednateli a dále za ty, které se na díle vyskytnou v záruční době.

4. V případě, že objednatel nesdělí při vytknutí vady díla v rámci záruční doby zhotoviteli jiný požadavek, je zhotovitel povinen vytýkanou vadu nejpozději do 15 dnů poté, co mu bude oznámena, vlastním nákladem odstranit, přičemž pokud tak zhotovitel v plném rozsahu neučiní, má objednatel právo požadovat přiměřenou slevu z ceny díla či od smlouvy odstoupit. Další práva objednatele plynoucí mu z titulu vad díla ze smlouvy a obecně závazných právních předpisů tím nejsou dotčeny.

5. Zhotovitel je povinen využívat po celou dobu provádění díla projektový tým, jehož složení bude naplňovat minimálně technické kvalifikační požadavky zadávacího řízení předcházejícího uzavření smlouvy. Zhotovitel je oprávněn s předchozím písemným souhlasem objednatele měnit konkrétní osoby tvořící projektový tým, nicméně nová osoba musí výše uvedenou technickou kvalifikaci rovněž splňovat. Splnění technické kvalifikace musí zhotovitel doložit doklady, které měl v zadávacím řízení povinnost doložit před uzavřením této smlouvy (viz příloha č. 2 Seznam členů realizačního týmu).

6. Zhotovitel je povinen zachovávat mlčenlivost o veškerých skutečnostech, které se od objednatele dozvěděl nebo v budoucnu dozví v souvislosti s touto smlouvou. Zhotovitel

je povinen aktivně dbát o to, aby takové informace nebyly zneužity, nebo aby nedošlo k jejich prozrazení bez zákonného důvodu. Zhotovitel není povinen zachovávat mlčenlivost o informacích, ve vztahu, k nimž mu objednatel předem výslovně oznámí, že je nepovažuje za důvěrné.

7. Zhotovitel je povinen za účelem ověření plnění povinností vyplývajících ze smlouvy poskytnout součinnost a vytvořit podmínky k provedení kontroly vztahující se k realizaci projektu, poskytnout oprávněným osobám veškeré doklady vážící se k realizaci smlouvy, umožnit průběžné ověřování souladu uváděných údajů o realizaci smlouvy se skutečným stavem v místě její realizace a poskytnout součinnost všem osobám oprávněným k provádění kontroly. Těmito oprávněnými osobami jsou zaměstnanci a pověřené osoby objednatele, MPSV (Řídicí orgán), územní finanční orgány, Ministerstvo financí, Nejvyšší kontrolní úřad, Evropská komise a Evropský účetní dvůr, případně další orgány oprávněné k výkonu kontroly. Tato povinnost dodavatele trvá do 31. 12. 2033.

8. Zhotovitel má povinnost po skončení plnění předat veškeré potřebné dokumenty, které mají souvislost s plněním předmětu smlouvy zadavateli, který má povinnost je po stanovenou dobu archivovat.

9. Dílo dle smlouvy je prováděno v rámci projektu „SRUB – Strategický rozvoj Uherského Brodu 2022+" registrační číslo CZ.03.4.74/0.0/0.0/17_080/0010103. Tento projekt je realizován v rámci Operačního programu Zaměstnanost.

10. Veškeré vytvořené písemné výstupy musí obsahovat povinnou publicitu, tj. povinný prvek vizuální identity Operačního programu Zaměstnanost (tedy logolink uvedený v záhlaví smlouvy, případně na stránkách www.esfcr.cz) a název projektu „SRUB – Strategický rozvoj Uherského Brodu 2022".

11. Bude-li dílo obsahovat a pracovat s daty týkajícími se fyzických osob, zajistí zhotovitel, aby se v rámci v díle s relevantními daty pracovalo vždy důsledně v členění na data týkající se žen a mužů. Data, týkající se fyzických osob uváděná zejména v analytických částech dokumentů, budou členěna dle pohlaví tak, aby specifické potřeby obyvatel mohly být vhodně zohledněny v návrzích opatření. (To se týká například údajů o složení obyvatelstva daného území, statistiky o nezaměstnaných osobách, statistiky využívání veřejných služeb jako veřejná doprava, kulturní a sportovní zařízení a podobně). V případě, že data v členění dle pohlaví nejsou dostupná, případně jejich pořízení není možné v rámci projektu zajistit (bylo by to např. příliš časově nebo finančně náročné), uvede příjemce tuto skutečnost včetně příslušného zdůvodnění vhodným způsobem v dokumentu.

VIII. Závěrečná ustanovení

1. Smlouva nabývá platnosti podpisem poslední ze smluvních stran a účinnosti dnem jejího uveřejnění ve smyslu zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Objednatel v zákonné lhůtě odešle smlouvu k řádnému uveřejnění do registru smluv vedeného Ministerstvem vnitra ČR.

2. Smlouvu lze měnit pouze písemnými vzestupně číslovanými a oběma smluvními stranami podepsanými dodatky.

3. Smluvní strany shodně prohlašují, že obsah smlouvy není obchodním tajemstvím ve smyslu ustanovení § 504 občanského zákoníku, ve znění pozdějších předpisů a souhlasí

s případným zveřejněním jejího textu v souladu s ustanovením zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

4. K vyloučení všech pochybností smluvní strany prohlašují, že jsou jim známy účinky platného Obecného nařízení Evropského parlamentu a Rady (EU) 2016/679, ze dne 27. dubna 2016 (dále jen „Nařízení"). Zhotovitel je povinen zachovávat mlčenlivost o bezpečnostních opatřeních objednatele směřujících k ochraně osobních údajů. Při jakémkoliv nahodilém přístupu zhotovitele k osobním údajům v souvislosti s plněním smlouvy je zhotovitel povinen tyto údaje chránit, zejména znepřístupnit a nepředat údaje jiné osobě než objednateli.
5. Tato smlouva je podepsána elektronicky.
6. Nedílnou součástí této smlouvy je příloha č. 1 – Vymezení předmětu veřejné zakázky.
   příloha č. 2 – Seznam členů realizačního týmu

Schváleno orgánem obce:	Rada města Uherský Brod
	107. schůze konaná dne 13.01.2022, usnesení č. 2700/R107/22

V Uherském Brodě dne

Za objednatele
Město Uherský Brod

Ing. Ferdinand Kubáník, starosta

V Praze dne

Za zhotovitele
DoxoLogic, s.r.o.

Bc. Martin Listopad
Digitálně podepsal Bc. Martin Listopad
Datum: 2022.04.01 15:33:37 +04'00'

Bc. Martin Listopad, jednatel

příloha č. 1 – Vymezení předmětu veřejné zakázky

Dílčí plnění 1:

A. ETAPY PROJEKTU

1. Rozdílová analýza (identifikující úroveň plnění/neplnění standardů ISMS)

V první kroku je třeba zjistit stav jednotlivých oblastí řízení bezpečnosti informací na úřadě (respektive úroveň/míru implementace ISMS), k čemuž budou provedeny následující kroky:

- Provedení auditu managementu rizik (posouzení míry implementace řízení rizik z hlediska):
  - hodnocení, evidence a kontroly účinnosti řízení aktiv a rizik,
  - klasifikace, evidence, ochrany aktiv, manipulace s nimi, způsobu jejich používání atd.

- Definice rozsahu, tj. upřesnění procesních skupin (interesovaných subjektů), které mají být zkoumány:
  - posouzení úrovně zajištění organizační bezpečnosti,
  - posouzení kompetencí a povinností osob zastávajících bezpečnostní role:
    a. vlastníků/garantů aktiv (primárních),
    b. technických garantů aktiv (podpůrných),
    c. členů fóra/výboru kro kybernetickou a informační bezpečnost,
  - posouzení kompetencí a povinností administrátorů,
  - posouzení kompetencí a povinností zaměstnanců,

- posouzení kompetencí a povinností dodavatelů,
- identifikace procesních skupin,
- posouzení provázanosti výše uvedených subjektů v rámci procesních skupin.

- Určení odpovědných osob pro konzultace:
  - osob zastávajících bezpečnostní role (vlastníků/garantů aktiv),
  - administrátorů,
  - uživatelů (klíčových referentů),
  - dodavatelů (zajišťujících podporu a provoz aktiv).

- Auditování bezpečnostních procesů z pohledu vyspělosti:
  - existence procesu,
  - existence procesního vlastníka,
  - existence závazného standardu,
  - dodržování standardu, bezpečnostní povědomí zaměstnanců,
  - ověření v praxi pomocí auditních technik,
  - ověření existence kontrolních mechanismů.

Rozdílová analýza bude provedena v souladu s normou ČSN ISO/IEC 27001. Na základě zjištění z rozdílové analýzy bude stanovena vyspělost jednotlivých oblastí a identifikuje se soubor nedostatků vůči požadovaným ISMS standardům.

Výstupy etapy:

- **Rozdílová analýza**
  - Audit managementu rizik (řízení rizik a aktiv).
  - Matice procesních skupin a odpovědných osob.

- Audit bezpečnostních procesů.
- Souhrn naplněných a chybějících standardů ISMS.

2. Stanovení rozsahu systému (předmět řešení bezpečnosti informací – ISMS)

Definice rozsahu ISMS určuje, co bude předmětem řešení bezpečnosti informací (v úvahu se berou specifické rysy činností organizace, její struktura, umístění, aktiva a technologie apod.).

Jedná se o tzv. SCOPE (Co bude v rámci předmětu řešení bezpečnosti informací sledováno, de facto „jaké informace“ mají být chráněny a v „jakých systémech jsou obsaženy“).

Pro stanovení rozsahu ISMS je z hlediska „předmětu řešení ISMS“ nezbytné posouzení níže uvedených oblastí ISMS v návaznosti na kapitoly a s nimi souvisejí opatření dle ČSN ISO IEC 27001, a na jednotlivé § organizačních a technických opatření dle Vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti:

- systém řízení bezpečnosti informací,
- řízení rizik (aktiv),
- řízení organizační bezpečnosti (bezpečnostní role),
- bezpečnost lidských zdrojů,
- řízení přístupu,
- kryptografie,
- fyzická bezpečnost,
- řízení provozu a komunikací,
- akvizice vývoje a údržby systémů včetně dodavatelských vztahů,
- řešení kybernetických bezpečnostních událostí a incidentů,
- řízení kontinuity činností,
- řešení auditů a kontrol.

I přes obecné konstatování, že je potřeba chránit všechny informace, v praxi existuje řada omezení, která zaměří projekt na vybrané oblasti. Omezeními mohou být například investiční omezení, akutní potřeba řešit nejpalčivější problémy apod.

Pro stanovení priorit a omezení je potřeba definovat:

- Prioritní oblasti ISMS
- Omezující faktory z hlediska disponibilních prostředků:
    - finančních,
    - lidských zdrojů,
    - časových,
    - znalostních (odbornostních).

Výstupy etapy:

- **Předmět řešení ISMS (souhrn informačních systémů ISMS)**
    - Seznam vybraných provozních systémů ISMS.
    - Seznam vybraných agendových systémů ISMS.
    - Poskytované služby v rámci vybraných systémů ISMS.
    - Evidované a zpracovávané informace (+osobní údaje) u vybraných systémů ISMS.

- **Stanovení rozsahu systému** (v kontextu)
    - Bezpečnosti informací.
    - Organizace bezpečnosti informací.
    - Bezpečnosti lidských zdrojů.
    - Řízení aktiv.
    - Řízení přístupu.
    - Kryptografie.

- Fyzické bezpečnosti a bezpečnosti prostředí.
- Bezpečnosti provozu.
- Bezpečnosti komunikací.
- Akvizice, vývoje a údržby systémů.
- Vztahů s dodavateli.
- Řízení incidentů bezpečnosti informací.
- Aspektů řízení kontinuity činností organizace z hlediska bezpečnosti informací.
- Souladu s požadavky (předpisy, politiky, postupy, směrnice).

- **Procesní schéma rozsahu ISMS**
  - Prováděné činnosti
  - Role zúčastněných všech zúčastněných subjektů:
    - osob zastávajících bezpečnostní role,
    - fóra, výboru kybernetické bezpečnosti,
    - administrátorů,
    - zaměstnanců,
    - institucí (NÚKIB, ÚOOÚ, CERT).

- **Stanovení priorit a omezení**
  - Seznam prioritní oblasti ISMS
  - Seznam omezujících faktorů, „omezení“ pro implementaci ISMS:
    - finanční,
    - personální,
    - časové,

- znalostní,
- legislativní.

3. Definice Politiky ISMS, cílů a odpovědností

Politika ISMS je vrcholným dokumentem. Deklaruje vůli a chuť managementu úřadu se bezpečností informací zabývat, a také cíle, kterých chce organizace v této oblasti dosáhnout. Při vytváření Politiky ISMS je proto nezbytná úzká součinnost s managementem, tento dokument musí být jednomyslně přijat vrcholným vedením a následně se stát obecně závazným napříč celou organizací.

Seznam požadovaných bezpečnostních politik:

1.1. Politika systému řízení bezpečnosti informací

a) Cíle, principy a potřeby řízení bezpečnosti informací.

b) Rozsah a hranice systému řízení bezpečnosti informací.

c) Pravidla a postupy pro řízení dokumentace.

d) Pravidla a postupy pro řízení zdrojů a provozu systému řízení bezpečnosti informací.

e) Pravidla a postupy pro provádění auditů kybernetické bezpečnosti.

f) Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací.

g) Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací.

1.2. Politika řízení aktiv

a) Identifikace, hodnocení a evidence primárních aktiv.

b) Identifikace, hodnocení a evidence podpůrných aktiv.

c) Pravidla ochrany jednotlivých úrovní aktiv.

d) Způsoby spolehlivého mazání nebo ničení technických nosičů dat, informací, provozních údajů a jejich kopií.

1.3. Politika organizační bezpečnosti

a) Určení bezpečnostních rolí a jejich práv a povinností.

b) Požadavky na oddělení výkonu činností jednotlivých bezpečnostních rolí.

c) Požadavky na oddělení výkonu bezpečnostních a provozních rolí.

1.4. Politika řízení dodavatelů

a) Pravidla a principy pro výběr dodavatelů.

b) Pravidla pro hodnocení rizik souvisejících s dodavateli.

c) Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti.

d) Pravidla pro provádění kontroly zavedení bezpečnostních opatření.

e) Pravidla pro hodnocení dodavatelů.

1.5. Politika bezpečnosti lidských zdrojů

a) Pravidla rozvoje bezpečnostního povědomí a způsoby jeho hodnocení.

b) Bezpečnostní školení nových zaměstnanců.

c) Pravidla pro řešení případů porušení bezpečnostní politiky systému řízení bezpečnosti informací.

d) Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice.

1.6 Politika řízení provozu a komunikací

a) Pravomoci a odpovědnosti spojené s bezpečným provozem.

b) Postupy bezpečného provozu.

c) Požadavky a standardy bezpečného provozu.

d) Pravidla a omezení pro provádění auditů kybernetické bezpečnosti a bezpečnostních testů.

1.7. Politika řízení přístupu

a) Princip minimálních oprávnění/potřeba znát (need to know).

b) Požadavky na řízení přístupu.

c) Životní cyklus řízení přístupu.

d) Řízení privilegovaných oprávnění.

e) Řízení přístupu pro mimořádné situace.

f) Pravidelné přezkoumání přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách.

1.8. Politika bezpečného chování uživatelů

a) Pravidla pro bezpečné nakládání s aktivy.

b) Bezpečné použití přístupového hesla.

c) Bezpečné použití elektronické pošty a přístupu na internet.

d) Bezpečný vzdálený přístup.

e) Bezpečné chování na sociálních sítích.

f) Bezpečnost ve vztahu k mobilním zařízením.

1.9. Politika zálohování a obnovy a dlouhodobého ukládání

a) Požadavky na zálohování a obnovu.

b) Pravidla a postupy zálohování.

c) Pravidla a postupy dlouhodobého ukládání.

d) Pravidla bezpečného zálohování a dlouhodobého ukládání informací.

e) Pravidla a postupy obnovy.

f) Pravidla a postupy testování zálohování a obnovy.

g) Politika přístupu k zálohám, ukládaným informacím.

1.10. Politika bezpečného předávání a výměny informací

a) Pravidla a postupy pro ochranu předávaných informací.

b) Způsoby ochrany elektronické výměny informací.

c) Pravidla pro využívání kryptografické ochrany.

1.11. Politika řízení technických zranitelností

a) Pravidla pro omezení instalace programového vybavení.

b) Pravidla a postupy vyhledávání opravných programových balíčků.

c) Pravidla a postupy testování oprav programového vybavení.

d) Pravidla a postupy nasazení oprav programového vybavení.

1.12. Politika bezpečného používání mobilních zařízení

a) Pravidla a postupy pro bezpečné používání mobilních zařízení.

b) Pravidla a postupy pro zajištění bezpečnosti zařízení, která povinná osoba nemá ve své správě.

1.13. Politika akvizice, vývoje a údržby

a) Bezpečnostní požadavky pro akvizici, vývoj a údržbu.

b) Řízení zranitelností.

c) Politika poskytování a nabývání licencí programového vybavení a informací

1.14. Politika ochrany osobních údajů

a) Charakteristika zpracovávaných osobních údajů.

b) Popis přijatých a provedených organizačních opatření pro ochranu osobních údajů.

c) Popis přijatých a provedených technických opatření pro ochranu osobních údajů.

1.15. Politika fyzické bezpečnosti

a) Pravidla pro ochranu objektů.

b) Pravidla pro kontrolu vstupu osob.

c) Pravidla pro ochranu zařízení.

d) Detekce narušení fyzické bezpečnosti.

1.16. Politika bezpečnosti komunikační sítě

a) Pravidla a postupy pro zajištění bezpečnosti sítě.

b) Určení práv a povinností za bezpečný provoz sítě.

c) Pravidla a postupy pro řízení přístupů v rámci sítě.

d) Pravidla a postupy pro ochranu vzdáleného přístupu k síti.

e) Pravidla a postupy pro monitorování sítě a vyhodnocování provozních záznamů.

1.17. Politika ochrany před škodlivým kódem

a) Pravidla a postupy pro ochranu síťové komunikace.

b) Pravidla a postupy pro ochranu serverů a sdílených datových úložišť.

c) Pravidla a postupy pro ochranu pracovních stanic.

1.18. Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí

a) Pravidla a postupy nasazení nástroje pro detekci kybernetických bezpečnostních událostí.

b) Provozní postupy pro vyhodnocování a reagování na detekované kybernetické bezpečnostní události.

c) Pravidla a postupy pro optimalizaci nastavení nástroje pro detekci kybernetických bezpečnostních událostí.

1.19. Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí

a) Pravidla a postupy pro evidenci a vyhodnocení kybernetických bezpečnostních událostí.

b) Pravidla a postupy pravidelné aktualizace pravidel pro vyhodnocení kybernetických bezpečnostních událostí.

c) Pravidla a postupy pro optimální nastavení bezpečnostních vlastností nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí.

1.20. Politika bezpečného používání kryptografické ochrany

a) Úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu.

b) Pravidla kryptografické ochrany informací

c) Systém správy klíčů.

1.21. Politika řízení změn

a) Způsob a principy řízení významných změn v rámci povinné osoby, jejich procesech, informačních a komunikačních systémech.

b) Přezkoumávání dopadů významných změn.

c) Způsob vedení evidence a testování významných změn.

1.22. Politika zvládání kybernetických bezpečnostních incidentů

a) Definování kategorií kybernetického bezpečnostního incidentu.

b) Pravidla a postupy pro identifikaci, evidenci a zvládání jednotlivých kategorií kybernetických bezpečnostních incidentů.

c) Pravidla a postupy testování systému zvládání kybernetických bezpečnostních incidentů.

d) Pravidla a postupy pro vyhodnocení kybernetických bezpečnostních incidentů a pro zlepšování kybernetické bezpečnosti.

e) Evidence incidentů.

1.23. Politika řízení kontinuity činností

a) Práva a povinnosti zúčastněných osob.

b) Cíle řízení kontinuity činností

c) Politika řízení kontinuity činností pro naplnění cílů kontinuity.

d) Způsoby hodnocení dopadů kybernetických bezpečnostních incidentů na kontinuitu a posuzování souvisejících rizik.

e) Určení a obsah potřebných plánů kontinuity a havarijních plánů.

f) Postupy pro realizaci opatření vydaných Úřadem.

Nezbytnou součástí této fáze je také definování osoby/osob s primární zodpovědností za bezpečnost informací v rozsahu:

- osob zastávajících bezpečnostní role
- výboru kybernetické bezpečnosti
- administrátorů
- zaměstnanců

Výstupy etapy:

- **Zpracována bezpečnostní politika**

1. Politika systému řízení bezpečnosti informací
2. Politika řízení aktiv
3. Politika organizační bezpečnosti
4. Politika řízení dodavatelů
5. Politika bezpečnosti lidských zdrojů
6. Politika řízení provozu a komunikací
7. Politika řízení přístupu
8. Politika bezpečného chování uživatelů
9. Politika zálohování a obnovy a dlouhodobého ukládání
10. Politika bezpečného předávání a výměny informací
11. Politika řízení technických zranitelností
12. Politika bezpečného používání mobilních zařízení
13. Politika akvizice, vývoje a údržby
14. Politika ochrany osobních údajů
15. Politika fyzické bezpečnosti
16. Politika bezpečnosti komunikační sítě
17. Politika ochrany před škodlivým kódem
18. Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí
19. Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí
20. Politika bezpečného používání kryptografické ochrany
21. Politika řízení změn

22. Politika zvládání kybernetických bezpečnostních incidentů
23. Politika řízení kontinuity činností

- **Cíle ISMS**

Naplnění cílů ISMS, jejich specifikace a provázanost na bezpečnostní politiky z hlediska:

- zajištění bezpečnosti informačních a komunikačních systémů a služeb,
- zajištění kontinuity provozu informačních a komunikačních systémů a služeb,
- ochrany dat a informací, a dalších aktiv,
- řešení hrozeb, událostí a incidentů včetně prevence,
- zvyšování bezpečnosti informačních a komunikačních systémů a služeb,
- zvyšování obecného podvědomí uživatelů o bezpečnosti a bezpečnostních hrozbách (edukace),
- sdílení zkušeností s dalšími subjekty.

- **Jmenovací listina osoby/osob s primární zodpovědností za bezpečnost informací**
  - osoby zastávající bezpečnostní role
  - osoby v rámci fóra/výboru kybernetické bezpečnosti
  - osoby / administrátoři

4. Analýza rizik

Analýza rizik je klíčovou aktivitou při budování bezpečnosti informací. Cílem je odpovědět na následující otázky:

- Jakými způsoby může být v naší organizaci porušena bezpečnost informací?
- Jaká je pravděpodobnost, že se to stane?

- Jaké budou dopady na organizaci (případně její okolí, nebudou-li informace chráněny?

V rámci analýzy rizik dojde k zaměření na hrubou analýzu procesů požadovaných normou ISO 27001 v součinnosti především s vlastníky procesů, resp. vedoucími pracovníky úřadu. Samotný proces analýzy rizik zahrnuje identifikaci a hodnocení aktiv a identifikaci a stanovení pravděpodobností hrozeb a identifikaci a stanovení síly zranitelností.

a) Definice metodiky analýzy rizik

Před vlastní analýzou rizik je nutné stanovit a vedením úřadu schválit metodiku pro provádění

analýzy rizik. Tato metodika musí primárně vycházet z požadavků normy ISO 27001.
V rámci této metodiky bude stanoveno, jakým způsobem budou hodnocena aktiva a stanoveny míry rizika. Zároveň bude stanovena míra akceptace rizika, tedy od jaké hodnoty rizikovosti se bude jednat o akceptovatelné riziko bez následných opatření a od jaké hodnoty jsou nezbytná následná opatření směřující ke snížení rizika.
Stanovení přesné metodiky pro provádění analýzy rizik je předpokladem k tomu, aby analýza rizik byla v budoucnu opakovatelná. To umožní sledovat vývoj rizik v čase dle jednotné a stejné metodiky.

b) Identifikace a hodnocení aktiv

Hlavní pozornost bude věnována identifikaci a hodnocení jednotlivých aktiv (primárních a podpůrných). Hodnocení bude provedeno cestou interview s respondenty – odpovědnými představiteli uživatelů informačního systému (vedoucími pracovníky) formou ocenění následků ztráty dostupnosti, důvěrnosti a integrity podle předem připravených scénářů „Co se stane, když...".

c) Hodnocení hrozeb a zranitelnosti

Hodnocení hrozeb a zranitelnosti je rovněž formální proces spočívající v zodpovězení sady předem připravených otázek vycházejících z požadavků norem ISO 27001 a ISO 27005.

d) Hodnocení rizik a vytvoření souboru opatření

Míra rizika bude stanovena pro jednotlivé prvky modelu aktiv (primární aktiva ve smyslu informací a služeb, podpůrná technická aktiva) jako součin hodnoty aktiv, pravděpodobnosti hrozeb a síly zranitelnosti. Vypočítaná míra rizika je vyjádřena v relativní stupnici. Zároveň je vygenerován soubor (organizačních a technických) bezpečnostních opatření. Jednotlivá

bezpečnostní opatření jsou charakterizována bezpečnostní úrovní (ve stejné relativní stupnici jako míra rizika) a dalšími údaji, které umožní stanovit, na základě provedené analýzy rizik, prioritu (naléhavost) jejich realizace. Zjištěná rizika budou srozumitelně popsána, včetně jejich souvislostí s určitými aktivy, hrozbami a zranitelností.

e) Návrhy a doporučení – aplikace analýzy

V závěrečné fázi budou vytvořeny návrhy na bezpečnostní opatření, případně rozhodnutí o akceptaci rizika, jejichž potřeba vyplyne z analýzy rizik. V rámci této fáze projektu budou navržena opatření organizačního charakteru, která nebudou představovat investice, případně jiné finanční náklady a technická opatření, která mohou být předmětem „zadání" projektů financovaných z Integrovaného regionálního operačního programu (IROP) v programovém období 2021–2027. Budou doporučeny priority a předložen návrh na další postup s ohledem na standardní etapy procesu řízení rizik a přijetí nezbytných manažerských rozhodnutí. Návrhy budou v dokumentu „Plán zvládání rizik" a podle potřeby doplněny v přílohách.

Výstupy etapy:

- **Metodika pro provádění analýzy rizik**
  - Metodika identifikace, klasifikace a hodnocení aktiv
    - Určení stupnice pro hodnocení primárních aktiv
      - určení stupnice pro hodnocení úrovní důvěrnosti aktiv,
      - určení stupnice pro hodnocení úrovní integrity aktiv,
      - určení stupnice pro hodnocení úrovní dostupnosti aktiv.
  - Metodika identifikace a hodnocení rizik
    - Určení stupnice pro hodnocení rizik
      - určení stupnice pro hodnocení úrovní dopadu,
      - určení stupnice pro hodnocení úrovní hrozby,
      - určení stupnice pro hodnocení úrovní zranitelnosti,
      - určení stupnice pro hodnocení úrovní rizik.
  - Metody a přístupy pro zvládání rizik

- Způsoby schvalování akceptovatelných rizik
- Proces hodnocení aktiv a rizik

- **Závěrečná zpráva z provedené analýzy rizik**
  - Vyhodnocení opatření z předchozího přezkoumání systému řízení bezpečnosti informací (ISMS).
  - Identifikace změn a okolností, které mohou mít vliv na ISMS.
  - Zpětná vazba o výkonnosti řízení bezpečnosti informací
    - neshody a nápravná opatření,
    - výsledky monitorování a měření,
    - výsledky auditu,
    - naplnění cílů systému řízení bezpečnosti informací.
  - Výsledky hodnocení rizik a stav plánu zvládání rizik.
  - Identifikace možností pro neustálé zlepšování.
  - Doporučení potřebných rozhodnutí, stanovení opatření a osob zajišťujících výkon jednotlivých činností.

- **Plán zvládání rizik**
  - Seznam identifikovaných rizik.
  - Zvládání rizik a návrh aplikovatelných opatření.
  - Plán realizace navržených opatření.

5. Bezpečnostní standardy (bezpečnostní dokumentace)

Bezpečnostní standardy (bezpečnostní dokumentace) navazují na bezpečnostní politiku (co, jak, proč a pro koho chránit atd.) a provedenou analýzu rizik.

Zahrnují kontrolní mechanismy jak technické, tak procedurální povahy. Jsou obvykle (v závislosti na zvoleném přístupu) zaměřeny na:

- Směrnice a postupy pro uživatele
- Směrnice a postupy pro správce IT/IS
- Postupy pro zachování kontinuity
- Postupy a směrnice pro monitorování systémů

a) Směrnice a postupy pro uživatele IS a správce IS

Formalizované dokumenty zahrnující postupy pro práci uživatelů a správců (administrátorů) tak, aby bylo dosaženo v bezpečnostní politice definovaných cílů. Je známo, že lidský faktor představuje potenciálně největší hrozbu pro bezpečnost informací. Lidé tedy nikdy nemohou být ve funkčním systému opomenuti.

Součástí zavádění standardů (dokumentace) v této oblasti nezbytně musí být provedeno seznámení dotčených subjektů (uživatelů a správců) s jednotlivými výstupy dokumentace (navazujících politik).

Standardy pro uživatele obvykle obsahují zásady pro používání a změny hesel, ochranu přenosných médií a počítačů, pravidla pro vynášení informací mimo úřad, pravidla pro přístup k informačním systémům z prostředí veřejného internetu, povinnosti související se zjištěním bezpečnostních incidentů apod.

Směrnice a postupy pro uživatele navazují na konkrétní bezpečnostní politiky (stanovující povinnosti a pravidla zejména v oblasti bezpečného chování uživatelů, používání kryptografické ochrany a mobilních zařízení, zvládání kybernetických bezpečnostních incidentů atd.)

Směrnice a postupy pro správce IS (administrátory) navazují na konkrétní bezpečnostní politiky (definující povinnosti a pravidla zejména v oblasti zajištění bezpečnosti z hlediska řízení provozu a komunikací, řízení přístupu, zálohování a obnovy, akvizice a vývoje IS, komunikační sítě, fyzické bezpečnosti, ochrany před škodlivým kódem, zvládání kybernetických bezpečnostních incidentů atd.)

b) Směrnice pro plánování kontinuity

Tato směrnice bude obsahovat závazná pravidla pro to, jakým způsobem předcházet vzniku

nepříznivých situací, které by mohly ovlivnit chod organizace a bude definovat pravidla pro tvorbu havarijních plánů na základě provedené detailní analýzy rizik a analýzy dopadů.

c) Monitorování systémů

Postupy a směrnice pro monitorování systémů definují, které informace, ukazatele, výstrahy

systémů apod. je potřeba monitorovat, jak často a jakým způsobem. Úkolem je podchytit indikace možných výpadků, nelegální činnosti v informačním systému atd. a umožnit tak rychlé řešení potenciální hrozby.

Výstupy etapy:

- **Struktura dokumentace**
  - návrh jednotné struktury dokumentace, řízení dokumentace.

- **Směrnice a postupy pro uživatele IS**
  - změny hesel,
  - ochrana přenosných médií a počítačů,
  - pravidla pro vynášení informací mimo úřad,
  - pravidla pro přístup k informačním systémům z prostředí veřejného internetu,
  - povinnosti související se zjištěním bezpečnostních incidentů atd.

- **Směrnice a postupy pro správce IS**
  - řízení provozu a komunikací,
  - řízení přístupu,
  - pravidla pro zálohování a obnovu,
  - povinnosti v rámci akvizice a vývoje IS,
  - pravidla pro zajištění bezpečnosti komunikační sítě,
  - povinnosti v rámci fyzické bezpečnosti,

- pravidla pro ochranu před škodlivým kódem,
- povinnosti související se zvládáním kybernetických bezpečnostních incidentů atd.

- **Směrnice pro plánování kontinuity**
  - Plán kontinuity činností
    - cíle řízení kontinuity činností,
    - role zaměstnanců v procesu řízení kontinuity činností,
    - podíl dodavatelů v procesu řízení kontinuity činností,
    - plány řízení kontinuity činností,
    - implementace řízení kontinuity činností.
  - Plán zálohy
    - vazba na bezpečnostní politiku
    - popis činností a postupů v procesu zálohování,
    - popis kontrolních mechanismů v procesu zálohování,
    - podíl zaměstnanců na procesu zálohování,
    - podíl správců na procesu zálohování,
    - podíl dodavatelů na procesu zálohování,
    - popis použití zálohy při obnově.
  - Plán obnov
    - vazba na bezpečnostní politiku
    - popis činností a postupů v procesu obnovy,
    - popis kontrolních mechanismů v procesu obnovy,
    - podíl zaměstnanců na procesu obnovy,
    - podíl správců na procesu obnovy,

- podíl dodavatelů na procesu obnovy.

- **Monitorování systémů**
  - Směrnice pro řešení bezpečnostních událostí
    - navazující bezpečnostní politiky, metodiky,
    - definování pravidel a postupů pro:
      - detekci, evidenci bezpečnostních událostí,
      - zpracování záznamů vzniklých bezpečnostních událostí.
    - popis procesů řízení událostí v průběhu fází (sběru, ukládání, archivace, analýzy, posouzení dopadů na aktiva, aplikace vhodného bezpečnostního opatření, vyhodnocení a posouzení, zda jde o bezpečnostní incident)
  - Směrnice pro zvládání bezpečnostních incidentů
    - navazující bezpečnostní politiky, metodiky
    - definování pravidel a postupů,
    - přijmutí opatření pro jejich odvrácení a zmírnění dopadu,
    - šetření a odstranění příčiny vzniku a následků,
    - hlášení NBÚ a zaznamenávání celého průběhu zvládání.

- **Prohlášení o aplikovatelnosti**
  - Přehled vyloučených bezpečnostních opatření požadovaných touto vyhláškou včetně zdůvodnění, proč nebyla aplikována.
  - Přehled zavedených bezpečnostních opatření včetně způsobu jejich implementace.

6. Doporučení k aktualizaci a údržbě bezpečnostní dokumentace a politik

Stanovení pravidel a definice nástrojů k ověřování trvalé kvality zavedeného systému managementu bezpečnosti informací za účelem trvalého a prokazatelného zajištění bezpečnosti informací.

Výstupy etapy:

- Předávací protokol o převzetí dokumentu s doporučeními, podepsaný Zadavatelem a Dodavatelem

7. Implementace ISMS

- Implementace jednotlivých opatření: V rámci této etapy budou do praxe zavedena organizační opatření definovaná v bezpečnostní dokumentaci, zejména v oblasti:
  - klasifikování a označování zpracovávaných informací
  - umístění (ukládání) důvěrných informací na bezpečné úložiště
  - změny nastavení bezpečnostní politiky IT apod.

- Rozvoj bezpečnostního povědomí uživatelů, administrátorů a osob zastávajících bezpečnostní role v oblasti požadavků systému managementu bezpečnosti informací (ISMS) zahrnující:
  - poučení pracovníků úřadu o bezpečnostní politice
  - poučení pracovníků úřadu o jejich povinnostech
  - poučení osob zastávajících bezpečnostní role o jejich odpovědnostech
  - školení ochrany informací pro vedoucí pracovníky
  - školení ochrany informací v rozsahu realizovaného projektu pro pracovníky

Výstupy etapy:

- Záznamy dokladující provedenou implementaci (vycházejí ze zavedené a schválené ISMS dokumentace/bezpečnostních standardů).

- Seznam proškolených uživatelů
- Seznam proškolených administrátorů
- Seznam proškolených osob zastávajících bezpečnostní role

8. Ověření připravenosti k certifikačnímu auditu

Prověření splnění povinností nutných k zahájení certifikačního auditu (formou výstupního auditu), v případě potřeby provedení nezbytných úprav v rozsahu výše uvedených plnění či jiných doporučení k dokončení připravenosti a poté vydání potvrzení o připravenosti k provedení certifikačního auditu.

Výstupy etapy:

- Potvrzení o připravenosti k provedení certifikačního auditu

9. Součinnost při procesu certifikace až do splnění účelu předmětu veřejné zakázky – získání certifikátu dle normy ČSN ISO/IEC 27001

Poskytnutí součinnosti nezbytné pro získání certifikátu dle připomínek a požadavků certifikující organizace, zahrnující zejména aktualizace dokumentů zpracovaných v rámci předmětu plnění, případně dopracování další požadované dokumentace, pomoc se zavedením stanoveného opatření, včetně provedení případných konzultací se zadavatelem.

Výstupy etapy:

- Předávací protokol obsahující seznam zapracovaných připomínek a požadavků certifikující organizace při aktualizaci dokumentů zpracovaných v rámci předmětu plnění, při dopracování potřebné dokumentace či zavedení opatření.

Dílčí plnění 2:

10. Zajištění certifikačního auditu implementovaného systému managementu bezpečnosti informací

Dodavatel v rámci předmětu plnění této dílčí části veřejné zakázky zajistí provedení certifikačního auditu implementovaného systému managementu bezpečnosti informací zadavatele od **nezávislého auditora** (který se nepodílel na dílčím plnění 1 - Zavedení systému ISO/ IEC 27001 - ISMS). Certifikačním auditem se pro účely této dílčí části veřejné zakázky rozumí všechny kroky certifikačního auditu, které je nezbytné absolvovat k získání platného certifikátu systému managementu bezpečnosti informací dle požadavků normy ČSN ISO/IEC 27001. Certifikát musí být vystaven certifikačním orgánem – procesním, akreditovaným národním akreditačním orgánem (pro Českou republiku ČIA) pro tuto oblast ověřování. Zadavatel stanovuje, že pro účely této zakázky vymezuje a požaduje provedení certifikace v lokalitě sídla Zadavatele.

Výstupy etapy:

- Doklad o zahájení certifikačního auditu osobou oprávněnou vystavit certifikát dle požadavků normy ČSN ISO/IEC 27001

11. Certifikace dle normy ČSN ISO/IEC 27001

Vystavení certifikátu shody s normou ČSN ISO/IEC 27001 certifikačním orgánem.

Výstupy etapy:

- Certifikát ČSN ISO/IEC 27001

B. HARMONOGRAM PROJEKTU

Dílčí plnění 1:

Fáze	Etapa	Termín (T = termín uzavření smlouvy)
Analytická část	12. Rozdílová analýza	T + 10 kalendářních dní
Analytická část	13. Stanovení rozsahu systému	T + 15 kalendářních dní

Analytická část	14. Definice Politiky ISMS, cílů a odpovědností	T + 30 kalendářních dní
Analytická část	15. Analýza rizik	T + 50 kalendářních dní
Návrhová část	16. Bezpečnostní standardy, bezpečnostní dokumentace	T + 80 kalendářních dní
Návrhová část	17. Doporučení k aktualizaci a údržbě bezpečnostních politik a dokumentace	T + 80 kalendářních dní
Realizační část	18. Implementace ISMS	T + 110 kalendářních dní
Realizační část	19. Ověření připravenosti k certifikačnímu auditu	T + 120 kalendářních dní
Realizační část	20. Součinnost při certifikačním procesu	T + 150 kalendářních dní

Dílčí plnění 2:

Fáze	**Etapa**	**Termín (T = termín uzavření smlouvy)**
Realizační část	21. Zajištění certifikačního auditu	T + 120 kalendářních dní
Realizační část	22. Certifikace dle normy ČSN ISO/IEC 27000	T + 150 kalendářních dní

Bc. Martin Listopad

Digitálně podepsal Bc. Martin Listopad
Datum: 2022.04.01 15:34:48 +04'00'

Příloha č. 2

Seznam členů realizačního týmu

Jméno a příjmení	Role
Ing. Kateřina Ketyiová	Vedoucí realizačního týmu
Bc. Pavel Duchan	Manažer informační bezpečnosti Auditor ISMS nebo QMS
Antonin Duong	Konzultant informační bezpečnosti
Laďka Šípková	Projektová koordinátorka

Bc. Martin Listopad

Digitálně podepsal Bc. Martin Listopad
Datum: 2022.04.01 15:35:20 +04'00'

.....

Bc. Martin Listopad
jednatel