



KUMSP00U45ZR

MORAVSKOSLEZSKÝ KRAJ – KRAJSKÝ ÚŘAD

ČÍSLO SMLOUVY (DODATKU) -1-

00407
poř. číslo2017
rokKŘ
zkr. odb.Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Veřejná zakázka 200/2017

**SMLOUVA O POSKYTOVÁNÍ SLUŽEB V OBLASTI ZAVEDENÍ ISMS
NA KRAJSKÉM ÚŘADĚ****I.****Smluvní strany****1. Moravskoslezský kraj**se sídlem: 28. října 117, 702 18 Ostrava
zastoupen: Ing. Tomáš KotyzaIČO: 70890692
DIČ: CZ70890692
bankovní spojení: Česká spořitelna, a. s.
číslo účtu: 160186-1650676349/0800

(dále jen „objednatel“)

a

2. Versa Systems s.r.o.se sídlem: Kosmova 665/10, Přívoz, 702 00 Ostrava
zastoupena: Ing. Václavem Štverkou, jednatelem společnosti
IČO: 25891863
DIČ: CZ25891863
bankovní spojení: ČSOB a.s., pobočka Ostrava
číslo účtu: 256448482/0300

Zapsána v obchodním rejstříku vedeném Krajským soudem v Ostravě, oddíl C, vložka 24491

(dále jen „poskytovatel“)

II.**Základní ustanovení**

1. Tato smlouva je uzavřena dle §1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“); práva a povinnosti stran touto smlouvou neupravená se řídí příslušnými ustanoveními občanského zákoníku.
2. Smluvní strany prohlašují, že údaje uvedené v čl. I této smlouvy jsou v souladu se skutečností v době uzavření smlouvy. Smluvní strany se zavazují, že změny dotčených údajů oznámí bez prodlení písemně druhé smluvní straně. V případě změny účtu poskytovatele je poskytovatel povinen rovněž doložit vlastnictví k novému účtu, a to kopií příslušné smlouvy nebo potvrzením peněžního ústavu. Při změně identifikačních údajů smluvních stran včetně změny účtu není nutné uzavírat ke smlouvě dodatek.
3. Je-li poskytovatel plátcem daně z přidané hodnoty (dále jen „DPH“), prohlašuje, že bankovní účet uvedený v čl. I odst. 2 této smlouvy je bankovním účtem zveřejněným ve smyslu zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „zákon o DPH“). V případě změny účtu poskytovatele je poskytovatel povinen doložit vlastnictví k novému účtu, a to

A1

kopii příslušné smlouvy nebo potvrzením peněžního ústavu; je-li poskytovatel plátcem DPH, musí být nový účet zveřejněným účtem ve smyslu předchozí věty.

4. Smluvní strany prohlašují, že osoby podepisující tuto smlouvu jsou k tomuto jednání oprávněny.
5. Poskytovatel prohlašuje, že je odborně způsobilý k zajištění předmětu plnění podle této smlouvy.

III. Předmět smlouvy

1. Poskytovatel se zavazuje zajistit na svůj náklad a nebezpečí pro objednatele zavedení systému řízení bezpečnosti informací (ISMS - Information Security Management System), dále jen „ISMS“ v souladu s normou ČSN ISO/IEC 27001:2014, a nastavení řízení procesů spojených se zachováním dostupnosti, integrity a důvěrnosti informací na Krajském úřadě Moravskoslezského kraje. Zavedení systému ISMS zahrnuje tyto dílčí části:
 - a) úvodní přezkoumání připravenosti krajského úřadu na zavedení systému ISMS a stanovení jeho rozsahu,
 - b) informační seminář pro vedení krajského úřadu, vedoucí zaměstnance a pro zaměstnance,
 - c) přezkoumání a doplnění dokumentace dle požadavku normy,
 - d) implementace požadavků ISMS,
 - e) provedení interních auditů ISMS,
 - f) provedení kontrolních auditů s vazbou na kontrolu realizace nápravných a preventivních opatření a konečná kontrola projektu,
 - g) účast na certifikačním procesu,(dále také „služba“ nebo „služby“)

Bližší specifikace služeb je přílohou č. 1 této smlouvy.

Poskytovatel je oprávněn zahájit plnění služeb dle písm. b) – g) až po obdržení písemné výzvy k zahájení plnění těchto částí služeb.

2. Součástí předmětu plnění bude také zpracování harmonogramu realizace zavedení ISMS (dále jen „harmonogram“), který bude obsahovat popis dílčích aktivit nezbytných pro realizaci předmětu plnění; upřesnění času plnění, uvedení personálních požadavků na zaměstnance zhotovitele a objednatele (požadavky na součinnost). Poskytovatel je povinen návrh harmonogramu předložit **do 10 kalendářních dnů** ode dne nabytí účinnosti této smlouvy, nejpozději však na úvodním jednání realizačního týmu. Součástí harmonogramu bude vypracování soupisu „Požadavky na součinnost“, který bude obsahovat označení konkrétních osob jak ze strany objednavatele, tak ze strany poskytovatele, určených k realizaci plnění dle této smlouvy. Objednatel je oprávněn se k harmonogramu vyjadřovat, a to i opakovaně. Poskytovatel zpracuje připomínky objednatele k harmonogramu, a to i opakovaně. O předání harmonogramu bude vyhotoven předávací protokol.
3. Objednatel se zavazuje za provedené služby zaplatit poskytovateli cenu podle čl. IV této smlouvy.
4. Účelem této smlouvy je zavedení systému řízení bezpečnosti informací a ve spolupráci s objednavatelem dosažení shody systému řízení bezpečnosti informací s požadavky normy ČSN ISO/IEC 27001:2014.
5. Předpokládá se, že služby budou realizovány v rámci projektu „Kvalita a odborné vzdělávání zaměstnanců KÚ MSK“ CZ.03.4.74/0.0/0.0/16_058/0007372, v rámci Operačního programu Zaměstnanost (dále též „OPZ“).

IV. Cena za služby

1. Smluvní strany se dohodly na ceně plnění dle této smlouvy takto:

Označení služby	Cena bez DPH	DPH ve výši 21 %	Cena včetně DPH
dílčí část dle čl. III odst. 1 písm. a)	38 000 Kč	7 980 Kč	45 980 Kč
dílčí část dle čl. III odst. 1 písm. b)	20 000 Kč	4 200 Kč	24 200 Kč
dílčí část dle čl. III odst. 1 písm. c)	64 000 Kč	13 440 Kč	77 440 Kč
dílčí část dle čl. III odst. 1 písm. d)	144 000 Kč	30 240 Kč	174 240 Kč
dílčí část dle čl. III odst. 1 písm. e)	32 000 Kč	6 720 Kč	38 720 Kč
dílčí část dle čl. III odst. 1 písm. f)	24 000 Kč	5 040 Kč	29 040 Kč
dílčí část dle čl. III odst. 1 písm. g)	21 000 Kč	4 410 Kč	25 410 Kč
Celkem za služby	343 000 Kč	72 030 Kč	415 030 Kč

2. Cena za služby podle odst. 1 tohoto článku smlouvy zahrnuje veškeré náklady poskytovatele spojené se splněním jeho závazku z této smlouvy. Cena za služby je stanovena jako nejvýše přípustná a není ji možno překročit.
3. Je-li poskytovatel plátcem DPH, odpovídá za to, že sazba daně z přidané hodnoty bude stanovena v souladu s platnými právními předpisy; v případě, že dojde ke změně zákonné sazby DPH, je poskytovatel k ceně za služby bez DPH povinen účtovat DPH v platné výši. Smluvní strany se dohodly, že v případě změny ceny za služby v důsledku změny sazby DPH není nutno ke smlouvě uzavírat dodatek.

V. Místo a doba plnění

1. Poskytovatel je povinen poskytnout služby v místě plnění, kterým je Moravskoslezský kraj, Krajský úřad, 28. října 117, 702 18 Ostrava. Poskytovatel je povinen poskytnout služby (dílčí části) dle čl. III odst. 1 této smlouvy nejpozději **do 12 měsíců** ode dne nabytí účinnosti této smlouvy a v souladu s harmonogramem dle čl. III odst. 2 smlouvy.

VI. Způsob poskytnutí služeb

1. Služba (dílčí část) je provedena jejím řádným poskytnutím a potvrzením této skutečnosti objednatelem v protokolu o poskytnutí služeb (dílčí části), dále jen „protokol“.

Protokol bude obsahovat:

- název služby (příp. její části),
 - označení objednatele a poskytovatele,
 - číslo této smlouvy a datum jejího uzavření,
 - datum zahájení a dokončení služby (příp. její části),
 - datum a místo sepsání protokolu,
 - jména a podpisy zástupců objednatele a poskytovatele,
 - soupis poskytnutých služeb a prohlášení objednatele, zda s tímto soupisem souhlasí (nesouhlasí) a zda potvrzuje řádné provedení služby (příp. její části).
2. Poskytovatel a objednatel jsou oprávněni uvést v protokolu cokoli, co budou považovat za nutné.
3. Nebudou-li protokoly obsahovat údaje požadované v odst. 1 tohoto článku, je objednatel oprávněn odepřít podepsání a převzetí protokolu, a to až do předání protokolu s požadovanými údaji.

4. Před zahájením plnění dílčích částí dle čl. III odst. 1 písm. b), c), d), e), f) a g) odešle objednatel poskytovateli do 10 dnů od potvrzení řádně provedené služby (dílčí části) v předávacím protokolu výzvu k provedení dalších služeb (navazující dílčí části) dle této smlouvy. Výzva bude objednatelem zaslána na e-mail: versasys@versasys.cz Bez této výzvy objednatel není poskytovatel oprávněn zahájit plnění dalších služeb (navazující dílčí části). Pokud objednatel poskytovateli výzvu k zahájení plnění dalších částí služeb nezašle, má se za to, že objednatel plnění těchto dalších částí služeb nepožaduje.

VII.

Práva a povinnosti smluvních stran

1. Poskytovatel je povinen poskytnout služby v dohodnutém rozsahu, kvalitě a čase. Poskytované služby musí odpovídat příslušným právním předpisům, normám nebo jiné dokumentaci vztahující se k předmětu této smlouvy.
2. Poskytovatel se zavazuje písemně informovat objednatele o skutečnostech majících vliv na plnění této smlouvy, a to neprodleně, nejpozději následující pracovní den poté, kdy příslušná skutečnost nastane nebo poskytovatel zjistí, že by nastat mohla.
3. Pokud objednatel zjistí, že jsou služby poskytovány v rozporu s touto smlouvou, je povinen poskytovateli bez zbytečného odkladu tuto skutečnost písemně (popř. emailem) oznámit. Objednatel bude tyto skutečnosti oznamovat na:
 - a. e-mail: versasys@versasys.cz
 - b. adresu: Kosmova 665/10, 702 00 Ostrava, Přívoz
 - c. do datové schránky: 53b98m8
4. Objednatel je povinen poskytnout poskytovateli součinnost nutnou k provedení služeb.
5. Na základě výzvy objednatele učiněné ústně, telefonicky, písemně nebo e-mailem poskytovatel poskytne objednateli zprávu o stavu přípravy a realizaci plnění.
6. Poskytovatel se zavazuje poskytnout veškeré nezbytné informace a dokumentaci týkající se poskytování služeb dle této smlouvy za účelem kontroly, a to ze strany objednatele a jím pověřených osob, územních finančních orgánů, Ministerstva práce a sociálních věcí, Ministerstva financí, Nejvyššího kontrolního úřadu, Evropské komise a Evropského účetního dvora, případně dalších orgánů oprávněných k výkonu kontroly projektu. Ve vztahu k těmto kontrolním orgánům se poskytovatel zavazuje umožnit jim vstup do svých objektů a na své pozemky, zajistit dostupnost všech dokladů o průběhu poskytování služeb dle této smlouvy.
7. Poskytovatel se rovněž zavazuje umožnit všem subjektům oprávněným k výkonu kontroly projektu, z jejichž prostředků je plnění hrazeno, provést kontrolu dokladů souvisejících s plněním veřejné zakázky, a to po dobu danou právními předpisy ČR k jejich archivaci.
8. Poskytovatel se zavazuje řádně uchovávat veškeré originály účetních dokladů a originály dalších dokumentů souvisejících s realizací předmětu smlouvy po dobu 10 let od ukončení plnění dle této smlouvy, minimálně však do 31. 3. 2029. Doklady budou uchovány v souladu s platnými právními předpisy.
9. Poskytovatel je povinen dodržovat pravidla publicity OPZ a při zpracování a umístění log na všech dokumentech souvisejících s projektem se řídit Manuálem pro publicity, Manuálem vizuální identity OPZ v aktuálním znění a „Obecnou částí pravidel pro žadatele a příjemce v rámci Operačního programu zaměstnanost“ v aktuálním znění (viz <https://www.esfcr.cz/pravidla-pro-zadatele-a-prijemce-opz/-/dokument/797767>) a Corporate Design manuálem MSK (viz http://www.msk.cz/assets/publikace/manual_msk_2014_zkracena_verze.pdf).
10. Poskytovatel uhradí škodu, která objednateli vznikla plněním v rozporu s touto smlouvou, a to v plné výši. Poskytovatel rovněž objednateli uhradí náklady vzniklé při uplatňování práv z odpovědnosti za vady.
11. Poskytovatel se zavazuje zabezpečovat plnění dle této smlouvy prostřednictvím osob, jejichž prostřednictvím v rámci zadávacího řízení na veřejnou zakázku prokázal splnění kvalifikačních požadavků a jejichž zkušenosti byly předmětem hodnocení v rámci zadávacího řízení, které

81

předcházelo uzavření této smlouvy. V případě změn jednotlivých osob je poskytovatel povinen vyžádat si písemný souhlas objednatele, tento souhlas vydá osoba oprávněna jednat za objednatele. Nové osoby musí disponovat minimálně stejnými zkušenostmi jako původní osoby, popřípadě minimálně zkušenostmi v takovém počtu, v jakém tyto zkušenosti prokázaly původní osoby, resp. alespoň v takovém počtu, který by neměl vliv na výsledné pořadí účastníků v zadávacím řízení. Objednatel vydá písemný souhlas se změnou do 5 dnů od doručení žádosti a potřebných dokladů, disponuje-li nová osoba potřebnými zkušenostmi. Objednatel nesmí souhlas se změnou osob bez objektivních důvodů odmítnout, pokud mu budou poskytovatelem příslušné doklady předloženy.

VIII.

Platební a fakturační podmínky

1. Úhrada ceny za služby bude provedena dle skutečného plnění služeb (dílčích částí) v návaznosti na poskytnutí služeb a potvrzení této skutečnosti objednatelem v souladu s čl. VI této smlouvy. Zálohové platby nebudou poskytovány.
2. Je-li poskytovatel plátcem DPH, podkladem pro úhradu ceny za služby budou faktury, které budou mít náležitosti daňového dokladu dle zákona o DPH a náležitosti stanovené dalšími obecně závaznými právními předpisy. Není-li poskytovatel plátcem DPH, podkladem pro úhradu ceny za služby budou faktury, která budou mít náležitosti účetního dokladu dle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů a náležitosti stanovené dalšími obecně závaznými právními předpisy. Faktury musí dále obsahovat:
 - a) číslo smlouvy objednatele, číslo veřejné zakázky (tj. 200/2017), IČO objednatele,
 - b) předmět smlouvy, tj. text „ Zavedení systému řízení bezpečnosti informací v souladu s normou ČSN ISO/IEC 27001:2014 a nastavení řízení procesů spojených se zachováním dostupnosti, integrity a důvěrnosti informací na Krajském úřadě“,
 - c) označení banky a číslo účtu, na který musí být zapláceno (pokud je číslo účtu odlišné od čísla uvedeného v čl. I odst. 2, je poskytovatel povinen o této skutečnosti v souladu s čl. II odst. 2 této smlouvy informovat objednatele),
 - d) lhůtu splatnosti faktury,
 - e) označení osoby, která fakturu vyhotovila, včetně jejího podpisu a kontaktního telefonu,
 - f) označení útvaru objednatele, který případ likviduje (odbor informatiky),
 - g) číslo protokolu o poskytnutí služeb a datum jeho podpisu. Protokol bude přílohou faktury.
3. Povinnost zaplatit cenu za služby je splněna dnem odepsání příslušné částky z účtu objednatele.
4. Lhůta splatnosti faktury činí 30 kalendářních dnů ode dne jejího doručení objednateli. Doručení faktury se provede osobně oproti podpisu zmocněné osoby objednatele nebo doručenkou prostřednictvím provozovatele poštovních služeb.
5. Nebude-li faktura obsahovat některou povinnou nebo dohodnutou náležitost nebo bude-li chybně vyúčtována cena nebo DPH, je objednatel oprávněn fakturu před uplynutím lhůty splatnosti vrátit druhé smluvní straně k provedení opravy s vyznačením důvodu vrácení. Poskytovatel provede opravu vystavením nové faktury. Vracením vadné faktury poskytovateli přestává běžet původní lhůta splatnosti. Nová lhůta splatnosti běží ode dne doručení nové faktury objednateli.
6. Je-li poskytovatel plátcem DPH, objednatel uplatní institut zvláštního způsobu zajištění daně dle § 109a zákona o DPH a hodnotu plnění odpovídající dani z přidané hodnoty uhradí v termínu splatnosti faktury stanoveném dle smlouvy přímo na osobní depozitní účet poskytovatele vedený u místně příslušného správce daně v případě, že:
 - a) poskytovatel bude ke dni poskytnutí úplaty nebo ke dni uskutečnění zdanitelného plnění zveřejněn v aplikaci „Registr DPH“ jako nespolehlivý plátec, nebo
 - b) poskytovatel bude ke dni poskytnutí úplaty nebo ke dni uskutečnění zdanitelného plnění v insolvenčním řízení, nebo
 - c) bankovní účet poskytovatele určený k úhradě plnění uvedený na faktuře nebude správcem daně zveřejněn v aplikaci „Registr DPH“.

Tato úhrada bude považována za splnění části závazku odpovídající příslušné výši DPH sjednané jako součást smluvní ceny za předmětné plnění. Objednatel nenese odpovědnost za případné penále a jiné postihy vyměřené či stanovené správcem daně poskytovateli v souvislosti s potenciálně pozdní úhradou DPH, tj. po datu splatnosti této daně.

IX.

Ochrana informací a osobních údajů

1. Poskytovatel je povinen zachovat jako citlivé veškeré informace, o kterých se dozví v souvislosti s plněním předmětu této smlouvy. Povinnost poskytovat informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, není tímto ustanovením dotčena.
2. Poskytovatel není oprávněn uvolnit, sdělit ani zpřístupnit jakékoliv třetí osobě informace objednatele bez jeho předchozího písemného souhlasu, a to v jakékoliv formě, a je povinen podniknout veškeré kroky nezbytné k zabezpečení daných informací. Povinnost zachovávat mlčenlivost a zajistit ochranu citlivých informací zůstává v platnosti neomezeně dlouho i po ukončení platnosti a účinnosti této smlouvy.
3. Poskytovatel je povinen zabezpečit veškeré podklady, mající charakter citlivé informace, poskytnuté mu objednatelem, proti odcizení nebo jinému zneužití.
4. Poskytovatel je povinen svého případného poddodavatele zavázat povinností mlčenlivosti a respektováním práv objednatele nejméně ve stejném rozsahu, v jakém je v závazkovém vztahu povinen sám. Za porušení povinnosti zachovávat mlčenlivost a zajistit ochranu citlivých informací poddodavatelem odpovídá objednateli přímo poskytovatel.
5. Povinnost zachovávat mlčenlivost se nevztahuje na informace:
 - které jsou nebo se stanou všeobecně a veřejně přístupnými jinak, než porušením ustanovení tohoto článku smlouvy ze strany poskytovatele,
 - které jsou poskytovateli známy a byly mu volně k dispozici ještě před přijetím těchto informací od objednatele,
 - které budou následně poskytovateli sděleny bez závazku mlčenlivosti vůči třetí osobě, jež rovněž není ve vztahu k nim nijak vázána,
 - jejichž sdělení vyžadují platné a účinné právní předpisy.
6. Poskytovatel se zavazuje, že důvěrné informace jiným subjektům nesdělí, nezpřístupní, ani nevyužije pro sebe nebo pro jinou osobu. Zavazuje se zachovat je v přísné tajnosti a sdělit je výlučně těm svým zaměstnancům nebo poddodavatelům, kteří jsou pověřeni plněním této smlouvy a za tímto účelem jsou oprávněni se s těmito informacemi v nezbytném rozsahu seznámit. Poskytovatel se zavazuje zabezpečit, aby i tyto osoby považovaly uvedené informace za důvěrné a zachovávaly o nich mlčenlivost. Za porušení povinnosti zachovávat mlčenlivost a zajistit ochranu citlivých informací poddodavatelem či zaměstnanci poskytovatele odpovídá objednateli přímo poskytovatel.
7. V případě, že bude při plnění předmětu této smlouvy docházet ke zpracování osobních údajů, je tato smlouva zároveň smlouvou o zpracování osobních údajů ve smyslu § 6 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „ZOOÚ“). Poskytovatel má pro účely ochrany osobních údajů postavení zpracovatele ve smyslu ZOOÚ.
8. Poskytovatel je oprávněn zpracovávat osobní údaje pouze za účelem plnění předmětu a účelu této smlouvy.
9. Poskytovatel je oprávněn zpracovávat osobní údaje v rozsahu nezbytně nutném pro plnění této smlouvy, za tímto účelem je oprávněn osobní údaje zejména ukládat na nosiče informací, upravovat, uchovávat po dobu nezbytnou k uplatnění práv zhotovitele vyplývajících z této smlouvy, předávat zpracované osobní údaje objednateli, osobní údaje likvidovat.
10. Poskytovatel učiní v souladu s platnými právními předpisy dostatečná organizační a technická opatření zabraňující přístupu neoprávněných osob k osobním údajům o ochraně osobních údajů.
11. Poskytovatel zajistí, aby jeho pracovníci byli v souladu s platnými a účinnými právními předpisy poučeni o povinnosti mlčenlivosti a o možných následcích pro případ porušení této povinnosti.

12. Poskytovatel zajistí, aby písemnosti a jiné hmotné nosiče informací, které obsahují citlivé údaje, byly uchovávány v uzamykatelných skříních umístěných v uzamykatelných místnostech.
13. Poskytovatel zajistí, aby elektronické datové soubory obsahující osobní údaje byly uchovávány v paměti počítače či jiného zařízení pouze:
 - je-li přístup k takovýmto souborům chráněn heslem,
 - je-li přístup k užívání počítače či jiného zařízení, v jehož paměti jsou tyto soubory umístěny, chráněn heslem.
14. Je-li pro účely této smlouvy nezbytné poskytnout poskytovateli kopii databází, souborů nebo nosičů údajů obsahujících jakékoliv údaje o činnosti objednatele a jím určených organizací, je poskytovatel povinen s takovými údaji nakládat tak, aby nedošlo k jejich úniku či zneužití.
15. Povinnost ochrany důvěrných informací trvá bez ohledu na ukončení účinnosti této smlouvy.
16. Vzhledem k veřejnoprávnímu charakteru objednatele, poskytovatel výslovně prohlašuje, že je s touto skutečností obeznámen a souhlasí se zveřejněním smluvních podmínek obsažených v této smlouvě v rozsahu a za podmínek vyplývajících z příslušných právních předpisů, zejména zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů a zákona č. 134/2016 Sb., o zadávání veřejných zakázek.

X.

Práva z vadného plnění

1. Služba není poskytnuta bezvadně, jestliže nebyla poskytnuta dle požadavků uvedených v této smlouvě.
1. Vadné plnění bude poskytovatelem odstraněno bezplatně, resp. bude bezplatně provedeno plnění bezvadné.
2. Veškerá vadná plnění (dále jen „vady“) je objednatel povinen uplatnit u poskytovatele bez zbytečného odkladu poté, kdy vadu zjistil, a to formou písemného oznámení (popř. e-mailem), obsahujícím co nejpodrobnější specifikaci zjištěné vady. Objednatel bude vady oznamovat na:
 - a. e-mail: versasys@versasys.cz
 - b. adresu: Kosmova 665/10, 702 00 Ostrava, Přívoz
 - c. do datové schránky: 53b98m8
3. Je-li vadné plnění podstatným porušením smlouvy, má objednatel také právo od smlouvy odstoupit.
4. Poskytovatel je povinen odstranit vadu nejpozději do 5 dnů od jejího oznámení objednatelem, pokud se smluvní strany v konkrétním případě nedohodnou písemně jinak.
5. Poskytovatel je povinen uhradit objednateli škodu, která mu vznikla vadným plněním, a to v plné výši. Poskytovatel rovněž objednateli uhradí náklady vzniklé při uplatňování z vadného plnění.

XI.

Sankce

1. V případě, že poskytovatel neposkytne služby (dílčí část) včas, je povinen zaplatit objednateli smluvní pokutu ve výši 0,5 % z ceny za příslušnou dílčí část bez DPH dle čl. IV odst. 1 této smlouvy, a to za každý započatý den prodlení.
2. Pokud poskytovatel neodstraní vadu ve lhůtě uvedené v čl. X odst. 4 této smlouvy, je povinen zaplatit objednateli smluvní pokutu ve výši 0,25 % z ceny za příslušnou dílčí část bez DPH dle čl. IV odst. 1 této smlouvy, a to za každý započatý den prodlení.
3. V případě nedodržení povinností poskytovatele dle čl. VII odst. 2 této smlouvy je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši 1.000 Kč, a to za každý zjištěný případ.
4. Pro případ prodlení se zaplacením ceny za služby sjednávají smluvní strany úrok z prodlení ve výši stanovené občanskoprávními předpisy.

5. Smluvní pokuty se nezapočítávají na náhradu případně vzniklé škody, kterou lze vymáhat samostatně vedle smluvní pokuty, a to v plné výši.
6. Provede-li poskytovatel změnu osob, jejichž prostřednictvím v rámci zadávacího řízení na veřejnou zakázku prokázal splnění kvalifikačních požadavků a jejichž zkušenosti byly předmětem hodnocení, v rozporu s čl. VII odst. 11 této smlouvy, je povinen zaplatit objednateli smluvní pokutu ve výši 10.000 Kč, a to za každý zjištěný případ.

XII. Zánik smlouvy

1. Smluvní strany se dohodly, že smlouva zaniká:
 - a) dohodou smluvních stran.
 - b) jednostranným odstoupením od smlouvy pro její podstatné porušení druhou smluvní stranou, přičemž podstatným porušením smlouvy se rozumí zejména:
 - neposkytnutí služeb (dílní části) ve stanoveném termínu,
 - neposkytnutí služeb v dohodnutém rozsahu a kvalitě,
 - nedodržení pokynů objednatele, právních předpisů nebo technických norem, které se týkají poskytování služeb,
 - nedodržení smluvních ujednání o právech z vadného plnění,
 - neuhrazení ceny za služby objednatelům po druhé výzvě poskytovatele k uhrazení dlužné částky, přičemž druhá výzva nesmí následovat dříve než 30 dnů po doručení první výzvy,
 - opakované porušení povinnosti poskytovatele dle čl. VII odst. 11 této smlouvy.
2. Objednatel je dále oprávněn od této smlouvy odstoupit v těchto případech:
 - a) bylo-li příslušným soudem rozhodnuto o tom, že poskytovatel je v úpadku ve smyslu zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů (a to bez ohledu na právní moc tohoto rozhodnutí);
 - b) podá-li poskytovatel sám na sebe insolvenční návrh;
 - c) že objednateli nebude přiznána dotace na projekt „Kvalita a odborné vzdělávání zaměstnanců KÚ MSK“ CZ.03.4.74/0.0/0.0/16_058/0007372 do 31. 3. 2018.
3. Pro účely této smlouvy se pod pojmem „bez zbytečného odkladu“ dle § 2002 občanského zákoníku rozumí „nejpozději do 3 týdnů“.

XIII. Závěrečná ustanovení

1. Tato smlouva nabývá platnosti a účinnosti dnem, kdy vyjádření souhlasu s obsahem návrhu smlouvy dojde druhé smluvní straně, nestanoví-li zákon 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 (dále jen „zákon o registru smluv“), jinak. V takovém případě nabývá smlouva účinnosti dnem jejího uveřejnění v registru smluv.
2. Doplnování nebo změnu této smlouvy lze provádět jen se souhlasem obou smluvních stran, a to pouze formou písemných, vzestupně číslovaných a takto označených dodatků.
3. Poskytovatel nemůže bez souhlasu objednatele postoupit svá práva a povinnosti plynoucí z této smlouvy třetí osobě.
4. Tato smlouva je vyhotovena v 5 stejnopisech s platností originálu, přičemž objednatel obdrží 4 a poskytovatel 1 její vyhotovení.
5. Smluvní strany se dohodly, že pokud se na tuto smlouvu vztahuje povinnost uveřejnění v registru smluv ve smyslu zákona o registru smluv, provede uveřejnění v souladu se zákonem objednatel.
6. V případě, že tato smlouva nebude uveřejněna dle předchozího odstavce, bere poskytovatel na vědomí a výslovně souhlasí s tím, že tato smlouva včetně příloh a případných dodatků bude

zveřejněna na oficiálních webových stránkách Moravskoslezského kraje. Smlouva bude zveřejněna po anonymizaci provedené v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

7. Nedílnou součástí této smlouvy je příloha č. 1 - Požadavky na zavedení ISMS na Krajském úřadě Moravskoslezského kraje.
8. Doložka platnosti právního jednání dle § 23 zákona č. 129/2000 Sb., o krajích (krajské zřízení), ve znění pozdějších předpisů:

K uzavření této smlouvy má objednatel souhlas rady kraje udělený usnesením č. 29/2534 ze dne 9. 1. 2018.

V Ostravě dne: 09 .07. 2018

V Ostravě dne: 22. 7. 2018



za objednatele
Ing. Tomáš Kotyza
ředitel krajského úřadu



za poskytovatele
Ing. Václav Štverka
jednatel společnosti



Příloha č. 1. Požadavky na zavedení ISMS na Krajském úřadě Moravskoslezského kraje

Cíl projektu:

Cílem projektu je zavedení systému řízení bezpečnosti informací (ISMS - Information Security Management System), dále jen „ISMS“, v souladu s normou ČSN ISO/IEC 27001:2014, a nastavení řízení procesů spojených se zachováním dostupnosti, integrity a důvěrnosti Informací na Krajském úřadě Moravskoslezského kraje (dále jen „krajský úřad“).

Popis zadání jednotlivých etap projektu:

1) Harmonogram realizace

2) Harmonogram bude obsahovat popis dílčích aktivit nezbytných pro realizaci díla (viz body 2 až 7 „Zavedení systému ISMS na Krajském úřadě Moravskoslezského kraje“) s upřesněním času plnění.

Úvodní přezkoumání připravenosti krajského úřadu na zavedení systému ISMS a stanovení jeho rozsahu

Cílem úvodního přezkoumání je zjistit míru připravenosti krajského úřadu na zavedení systému ISMS. Z úvodního přezkoumání bude vypracována zpráva popisující mimo jiné stav bezpečnosti informací na krajském úřadě a návrh na realizaci doporučení (opatření) vedoucích k dosažení shody s požadavky normy ČSN ISO/IEC 27001:2014 a zákona č. 181/2014 Sb., zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „zákon o kybernetické bezpečnosti“ nebo „ZoKB“). Dalším výstupem úvodního přezkoumání bude formalizovaný dokument obsahující definovaný rozsah zaváděného systému ISMS včetně zvolené strategie a cílů.

Součástí úvodního přezkoumání bude:

- Zpracování rozdílové analýzy připravenosti krajského úřadu na požadavky zákona o kybernetické bezpečnosti.
- Zhodnocení stávající situace v oblasti správy informačních rizik, řízení rizik a ICT bezpečnosti.
- Identifikace průnikových parametrů a procesů mezi již zavedenou normou ČSN EN ISO 9001, ČSN EN ISO14001, zákonem o kybernetické bezpečnosti a návrhu procesů v souladu s normou ČSN ISO/IEC 27001:2014.
- Zpracování stanovení návrhu rozsahu a hranice ISMS, definování kontextu včetně externího a interního aspektu ISMS (dle kap. 4 ČSN ISO/IEC 27001) tak, aby bylo reálné ISMS implementovat v podmínkách krajského úřadu. Kontext musí být v souladu s požadavky ISO 27001 a také s požadavky kybernetického zákona.
- Přezkoumání bezpečnostních politik, kontrola nastavení stávající metodiky pro vyhledávání a hodnocení rizik, sledování konzistence odpovědností a pravomocí v oblasti informační bezpečnosti.
- Přezkoumání evidence informačních aktiv včetně podpůrných aktiv dle zákona o kybernetické bezpečnosti a jejich vlastníků (garantů) a jejich zdokumentování včetně určení významnosti aktiv.
- Přezkoumání existujících hrozeb pro informační aktiva a zranitelnosti, které by mohly být hrozbami využity, přezkoumání zmapování dopadů na aktiva z hlediska ztráty důvěrnosti, integrity a dostupnosti.
- Přezkoumání posouzení pravděpodobnosti selhání bezpečnosti včetně následků na ztrátu důvěrnosti, integrity a dostupnosti aktiv.
- Přezkoumání odhadu úrovně rizik a analýza, zdali jsou bezpečnostní rizika akceptovatelná nebo vyžadují opatření pro jejich minimalizaci.
- Přezkoumání stavu identifikace variant pro zvládnutí rizik.
- Přezkoumání rizikových scénářů a možných souvisejících hrozeb.
- Přezkoumání, zda rámce řízení informačních rizik odpovídají standardu ZoKB.
- Zpracování analýzy a doplnění cílů a opatření dle přílohy A normy ČSN ISO/IEC 27001:2014 včetně Prohlášení o aplikovatelnosti.
- Přezkoumání existence souhlasu vedení krajského úřadu se zbytkovými riziky.
- Přezkoumání způsobu přidělování hesel a přihlašování do systému.
- Přezkoumání dokumentace a nastavení procesů u technické vybavenosti, technické shody a identifikace technických zranitelností v IT infrastruktuře krajského úřadu IT specialistů pro bezpečnost HW dle ZOKB.

- Zdokumentování postupu pro včasnou detekci pokusů o narušení bezpečnosti z oblasti IT včetně přezkoumání nastavení tohoto postupu.
- Přezkoumání dokumentovaného hodnocení rizik včetně zbytkových rizik s ohledem na případné změny kontextu organizace, identifikované hrozby a účinnost zavedených opatření.
- Přezkoumání způsobu zaznamenávání bezpečnostních incidentů a zpracovaného bezpečnostního plánu.
- Přezkoumání povinných dokumentovaných postupů dle ČSN ISO/IEC 27001:2014.

3) Informační seminář pro vedení krajského úřadu, pro vedoucí zaměstnance a zaměstnance

Provedení informačního semináře v oblasti ISMS, který bude zaměřen svým obsahem a rozsahem pro vedení krajského úřadu, vedoucí zaměstnance a zaměstnance. Semináře budou probíhat v objektu krajského úřadu za pomoci vizualizace (např. VT, dataprojektor, apod.). Součástí informačního semináře bude osvědčení o účasti.

V rámci tohoto bodu bude vypracována osnova semináře a harmonogram realizace semináře, včetně zpracování pozvánky pro jednotlivé účastníky. Součástí semináře budou také praktické příklady a řešení jednotlivých vzorových situací z řízení ISMS na krajském úřadě.

Minimální obsah semináře:

- Přínosy implementace systémů řízení, včetně ISMS
- Právní a technická regulace bezpečnosti informací v oblastech:
 - systému řízení bezpečnosti informací (ISMS) ve smyslu ISO 27001:2014
 - Zákon 365/2000 Sb., o informačních systémech veřejné správy (dále jen „zákon o ISVS“)
 - Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- Přehled bezpečnostních opatření ISMS

a) Informační seminář pro zaměstnance (cca 610)

- Předpokládaný rozsah semináře 2 hodiny: 1 hodina výklad, 1 hodina řízená diskuze k dotazům účastníků
- Vytvoření prezentace, která bude sloužit jako podklad pro informační seminář pro zaměstnance.

b) Informační seminář pro vedoucí zaměstnance (cca 65)

- Rozsah semináře 2 hodiny: 1 hodina výklad, 1 hodina řízená diskuze k dotazům účastníků

c) Informační seminář pro vedení krajského úřadu (cca 10 osob)

- Rozsah semináře 2 hodiny: 1 hodina výklad, 1 hodina řízená diskuze k dotazům účastníků

4) Přezkoumání a doplnění dokumentace dle požadavku normy ČSN ISO/IEC 27001:2014

V rámci této etapy bude provedeno přezkoumání, zhodnocení stávající dokumentace krajského úřadu s požadavky normy a zpracování relevantní dokumentace ISMS ve spolupráci s odpovědnými zaměstnanci krajského úřadu. Součástí této etapy projektu je i zapracování případných připomínek ze strany krajského úřadu do jednotlivých dokumentů a grafické zpracování a vydání dokumentace krajského úřadu v elektronické a tištěné podobě (min. ve dvou vyhotoveních ve formátu *.pdf. a *.docx).

Požadovaný minimální rozsah:

- Zpracování příručky ISMS do stávající příručky řízení objednavatele
- Prohlášení o aplikovatelnosti a souvisejících dokumentů

A.5	Politiky informační bezpečnosti informací
A.6	Organizace bezpečnosti informací
A.7	Bezpečnost lidských zdrojů
A.8	Management aktiv
A.9	Opatření k přístupu a řízení přístupových práv
A.10	Technologie kryptování

A.11	Fyzická bezpečnost pracovišť a zařízení
A.12	Bezpečnost provozu
A.13	Bezpečná komunikace a přenos dat
A.14	Bezpečná akvizice, vývoj a podpora informačních systémů
A.15	Bezpečnost pro dodavatele a třetí strany
A.16	Management incidentů
A.17	Kontinuita podnikání s ohledem na informační bezpečnost
A.18	Shoda s interními i externími požadavky

- Politika a cíle ISMS
- Metodika pro řízení rizik a plány zvládnání rizik
- Řízení informačních aktiv
- Plán kontinuity
- Řízení dokumentace a záznamů ISMS
- Řízení auditů ISMS
- Řízení nápravných opatření ISMS včetně zlepšování
- Řízení bezpečnostních incidentů
- Registr právních a jiných požadavků
- Zpracování bezpečnostních standardů a tvorby bezpečnostních dokumentů a směrnic, v rámci realizace směrnice budou vypracovány směrnice pro práci uživatelů s informačním systémem/informacemi a směrnice pro správu systému (rozsah je definován krajským úřadem, informačním systémem a identifikovanými riziky). Součástí tvorby bezpečnostních standardů je úprava potřebných dokumentů krajského úřadu, a její integrace do celkové koncepce krajského úřadu.
- Proces a směrnice ošetření přístupu třetích stran k informacím krajského úřadu.

5) Implementace požadavků ISMS

V rámci této etapy bude realizována implementační část, kdy budou zpracovány potřebné záznamy dle požadavků ISMS a k implementaci jednotlivých opatření vyplývajících z předchozí analýzy, zajišťujících dosažení požadovaného stupně informační bezpečnosti.

Dále bude provedena případná úprava zpracovaného harmonogramu pro implementaci ISMS, a to dle zjištění z úvodního přezkoumání připravenosti krajského úřadu na zavedení systému ISMS.

V rámci realizace projektu zadavatel požaduje minimálně 10 kontrolních dnů, na kterých bude prováděna kontrola postupu a metodické vedení implementace ISMS.

Implementační část zahrnuje:

- Zpracování evidence a monitorování informačních aktiv (primárních i podpůrných aktiv) včetně jejich vlastníků (garantů) a jejich zdokumentování a určení významnosti aktiv.
- Definování a vytvoření vazeb mezi aktivy včetně zpracování těchto vazeb do procesů systému řízení aktiv a řízení rizik ISMS.
- Provedení identifikace a zdokumentování existujících hrozeb pro informační aktiva a zranitelnosti, které by mohly být hrozbami využity, analýza zmapování dopadů na aktiva z hlediska ztráty důvěrnosti, integrity a dostupnosti. Posouzení pravděpodobnosti selhání bezpečnosti včetně následků na ztrátu důvěrnosti, integrity a dostupnosti aktiv. Odhad úrovně rizik a analýza, zda-li jsou bezpečnostní rizika akceptovatelná nebo vyžadují opatření pro jejich minimalizaci.
- Nastavení a monitorování identifikace variant pro zvládnání rizik jako je aplikace vhodných opatření, vědomé a objektivní akceptování rizik, vyhnutí se rizikům či přenesení rizik spojených s činností krajského úřadu na třetí strany.
- Nastavení, zdokumentování a sledování cílů a opatření dle přílohy A normy ČSN ISO/IEC 27001:2014. Definice cílů s přímou vazbou na informační aktiva a stanovení parametrů pro vyhodnocování cílů.
- Zpracování existence souhlasu vedení krajského úřadu se zbytkovými riziky včetně zpracování Prohlášení o aplikovatelnosti.
- Návrh variant pro zvládnání rizik, ve kterém vedení krajského úřadu vymezí odpovídající činnost vedení krajského úřadu, zdroje, odpovědnosti a priority pro ISMS.

- Nastavení postupů pro monitorování v:
 - Zavedených bezpečnostních opatřeních sloužících jako nástroje pro zvládání rizik, definování, jakým způsobem bude probíhat měření účinnosti vybraných opatření.
 - Zavedených programů školení a zvyšování informovanosti ve vztahu k ISMS.
 - Zavedení systému u přidělování hesel a přihlašování do systému ze vzdálených lokací.
 - Pravidla „prázdného stolu“.
 - Nastavení měření účinnosti zavedených opatření.
 - Nastavení zaznamenávání bezpečnostních incidentů.
 - Nastavení pravidelného přezkoumávání účinnosti ISMS s ohledem na výsledky bezpečnostních auditů, incidentů, výsledků měření účinnosti opatření, návrhů a podnětů všech zainteresovaných stran.
 - Nastavení a zdokumentování postupu pro včasnou detekci pokusů o narušení bezpečnosti z oblasti IT.
- Analýza procesů zvládání informačních incidentů s popisem slabých míst.
- Proškolení vybraných zaměstnanců, kteří následně budou provádět školení zaměstnanců krajského úřadu a zaměstnanců externích společností.

6) Provedení interních auditů ISMS

V této části projektu proběhnou na všech odborech krajského úřadu interní audity ISMS dle požadavku ČSN ISO IEC 27001: 2014 (čl. 9.2 a A. 12.7) v plném rozsahu normy ve spolupráci s interními auditory krajského úřadu. Cílem provedení interních auditů je ověření, zda zavedený systém řízení bezpečnosti informací vyhovuje požadavkům normy ČSN ISO/IEC 27001 a také požadavkům krajského úřadu. Nedílnou součástí interního auditu bude také verifikace provozních systémů.

Součástí interních auditů ISMS je zpracování programu auditů, plánu interních auditů, auditního dotazníku, zprávy z auditu dodavatelem ve spolupráci s interními auditory krajského úřadu a následné provedení kontrolních auditů pro uzavření zjištění z interního auditu.

7) Provedení kontrolních auditů s vazbou na kontrolu realizace nápravných a preventivních opatření a konečná kontrola projektu

Provedení kontrolních auditů pro odstranění neshod a realizace případných nápravných doporučení ve spolupráci se zaměstnanci krajského úřadu. Následně bude provedena konečná kontrola projektu a zpracována zpráva o stavu ISMS.

8) Účast na certifikačním procesu

Dodavatel se zúčastní auditu prvního a druhého stupně v rámci certifikačního procesu ISMS a poskytne odbornou pomoc při obhajobě zavedeného systému ISMS. V případě zjištěných nedostatků vypracuje dodavatel ve spolupráci s objednavatelem potřebné náležitosti vyplývající z uskutečněného certifikačního procesu, a to bezodkladně.

9) Dokumentace poskytnutá zadavatelem

- Bezpečnostní politika.
- Relevantní vnitřní předpisy a další akty interního řízení.
- Výstupy relevantních rizikových analýz a další nezbytné podklady, pokud má zadavatel zavedeny.

Veškeré aktivity vč. školení budou probíhat v českém jazyce, rovněž všechny výstupy (dokumenty apod.) budou v českém jazyce.

Handwritten signature