SML/2019/020

Níže uvedeného dne, měsíce a roku uzavřeli

Fakultní nemocnice Olomouc

státní příspěvková organizace zřízená Ministerstvem zdravotnictví ČR rozhodnutím ministra zdravotnictví ze dne 25.11.1990, č.j. OP-054-25.11.90
se sídlem: I. P. Pavlova 185/6, 779 00 Olomouc
IČ: 00098892
DIČ: CZ00098892
Zastoupená: prof. MUDr. Romanem Havlíkem, Ph.D., ředitelem
bankovní spojení: 36334811/0710

na straně jedné jako *„objednatel"*

a

ALEF NULA, a.s.

se sídlem: Pernerova 691/42, Karlín, 186 00 Praha 8
IČ: 61858579
DIČ: CZ61858579
zastoupená: Ing. Milanem Zinkem, předsedou představenstva
společnost je zapsaná v obchodním rejstříku Městského soudu v Praze, oddíl B., vložka 2727
bankovní spojení: Komerční banka, a.s. (51-3717150237/0100)

na straně druhé jako *„zhotovitel"*

(Uvedení zástupci obou stran prohlašují, že podle stanov nebo jiného obdobného organizačního předpisu jsou oprávněni tuto Smlouvu podepsat a k platnosti Smlouvy není třeba podpisu jiné osoby.)

tuto

SMLOUVU O DÍLO

I. Úvodní ustanovení

1. Zúčastněné smluvní strany si navzájem prohlašují, že jsou oprávněny tuto smlouvu uzavřít a řádně plnit závazky v ní obsažené, a že splňují veškeré podmínky a požadavky stanovené zákonem a touto smlouvou.

2. Tato smlouva je uzavírána na základě výsledků veřejné zakázky malého rozsahu zahájeného objednatelem jako veřejným zadavatelem s názvem **„Implementace zákona o kybernetické**

bezpečnosti a ISMS", evidenční číslo **VZ-2019-000345**. V případě, že je v této smlouvě odkazováno na zadávací dokumentaci, má se na mysli zadávací dokumentace vztahující se k uvedené veřejné zakázce.

II. Předmět smlouvy

1. Předmětem smlouvy je implementace zákona o kybernetické bezpečnosti č. 181/2014 Sb. (ZoKB) a systému řízení bezpečnosti informací (dále jen ISMS) v rámci rozsahu a hranic systému řízení informační bezpečnosti v prostředí ICT organizace, a to ve dvou fázích.

Fáze 1:

- Rozsah a hranice systému řízení informační bezpečnosti
  - vymezení z hlediska organizace - organizační rozsah dle organizační struktury, cílů
  - vymezení z hlediska řízených aktiv,
  - vymezení z hlediska informačních a komunikačních systémů
  - vymezení z hlediska fyzického rozsahu
  - doplnění / vyloučení

- Organizační role, odpovědnost a pravomoci v rámci ZoKB a ISMS
- Metodika hodnocení rizik
- Analýza rizik bezpečnosti informací (zahrnuje Identifikace a hodnocení aktiv)
- Návrh plánu ošetření rizik /zvládání rizik a Prohlášení o aplikovatelnosti (formalizace závěrů – vstup pro Risk registr, Management commitment, formalizace řešení rizik a přístup vedení pro řízení rizik)

Fáze 2:

- Bezpečnostní politika a Bezpečnostní a provozní dokumentace, návrh ISMS - organizace, role, odpovědnost
- Plán bezpečnostního vědomí zaměstnanců (školení, informovanost, odborná způsobilost)
- Interní audity a Přezkoumání ISMS
- Proces kontinuálního zlepšování
- Harmonizace a podpora přípravy organizace v dalších činnostech

Výstupem díla bude předání dokumentů dle předmětu Smlouvy v rozsahu definovaném přílohou č. 1. Součástí předmětu plnění je závazek Zhotovitele poskytnout po celou dobu trvání Smlouvy komplexní poradenské a konzultační služby, tvůrčí činnost Zhotovitele včetně hmotného zachycení jejího výsledku a poskytnutí výhradní licence k užití výsledků tvůrčí činnosti včetně jejího hmotného zachycení.
Předmět smlouvy – požadavky na obsah a rozsah plnění ve dvou fázích - je detailně popsán v příloze č. 1 této smlouvy.

2. Ukončení realizace předmětu Smlouvy je provedeno potvrzením akceptačního protokolu Objednatelem na základě předání díla dle čl. 2.1 Smlouvy Objednateli.
Po dohodě mezi Objednatelem a Zhotovitelem je možné převzít dílo i v případě, že je třeba dořešit minoritní funkční vady.

3. Výše uvedené dílo bude zpracováno řádně a včas na základě Objednatelem poskytnutých informací. Zhotovitel bude s Objednatelem přípravu výstupů průběžně konzultovat a koordinovat.

4. Veškeré odchylky od předmětu díla mohou být prováděny Zhotovitelem pouze tehdy, budou-li písemně odsouhlaseny Objednatelem, nestanoví-li tato smlouva jinak. Jestliže Zhotovitel provede práce a jiná plnění nad tento rámec, nemá nárok na jejich zaplacení, ledaže se smluvní strany písemně dohodnou nebo tato smlouva stanoví jinak.

III. Cena a platební podmínky

1. Cena za dílo dle čl. 2 Smlouvy je stanovena celkovou fixní částkou ve výši:

830 000 Kč bez DPH

174 300 Kč DPH

1 004 300 Kč včetně DPH

Pro účely částečné fakturace viz čl. III. 4 je Zhotovitel oprávněn celkovou částku rozdělit na:

- Akceptace a předání díla dle fáze 1. ve výši:

  310 000 Kč bez DPH

  65 100 Kč DPH

  375 100 Kč včetně DPH

- Akceptace a předání díla dle fáze 2. ve výši:

  520 000 Kč bez DPH

  109 200 Kč DPH

  629 200 Kč včetně DPH

2. Celková cena a ceny za jednotlivé fáze díla jsou cenami pevnými nejvýše přípustnými a zahrnují veškeré náklady, jejichž vynaložení je nutné na řádné a včasné splnění předmětu smlouvy, zejména náklady na dopravu, předání a veškeré náklady související, náklady na správní poplatky, daně, cla, schvalovací řízení, provedení předepsaných zkoušek, zabezpečení prohlášení o shodě, certifikátů a atestů, převod práv, pojištění, přepravních nákladů apod.

3. Cena je maximální a nemůže být navýšena ani v případě zvýšení sazby DPH.

4. Objednatel neposkytuje a Zhotovitel není oprávněn požadovat zálohy. Zhotovitel provádí fakturaci v souladu s čl. III odst. 1 této smlouvy na základě jím provedených a objednatelem převzatých plnění. Právo fakturovat má zhotovitel prvním dnem po akceptaci jednotlivých fází díla. Objednatelem budou prováděny platby za jednotlivé fáze díla, které budou osvědčeny akceptačními protokoly o předání a převzetí díla podepsanými oběma smluvními stranami.

5. Zhotovitel je povinen vystavit fakturu s náležitostmi daňového dokladu podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění a splatností 60 kalendářních dnů ode dne doručení faktury a nezbytnou přílohu faktury bude kopie akceptačního protokolu potvrzeného Objednatelem v souladu s příslušným ustanovením této smlouvy.

6. Zhotovitel je dále povinen, na faktuře, vystavené v rámci smluvního vztahu založeného touto smlouvou, uvést interní evidenční číslo **VZ-2019-000345.**

7. V případě, že faktura nebude splňovat veškeré náležitosti, je Objednatel oprávněn fakturu Zhotoviteli ve lhůtě splatnosti vrátit, přičemž lhůta splatnosti ceny začíná běžet znovu ode dne doručení řádně vystavené faktury Objednateli.

8. Cena bude Objednatelem uhrazena Zhotoviteli převodem na účet uvedený v záhlaví této smlouvy, případně na jiný účet uvedený v příslušné faktuře. Za den úhrady se rozumí den odeslání celé fakturované částky z účtu Objednatele na účet Zhotovitele.

IV. Doba plnění díla

1. Zhotovitel je povinen předat dílo Objednateli bez vad a nedodělků u dílčí fáze 1. nejpozději do 31. 10. 2019 a u dílčí fáze 2. nejpozději do 31.10.2021, a to v sídle Objednatele. Dílo bude realizováno dle harmonogramu, který tvoří nedílnou přílohu č. 2 této smlouvy. Zároveň se Zhotovitel zavazuje poskytovat Objednateli průběžně veškeré pracovní verze dokumentace, s minimální frekvencí – na vyžádání objednatele.

2. Termín plnění může být posunut. Posunutí termínu musí být odsouhlaseno statutárními zástupci obou smluvních stran formou písemného, chronologicky očíslovaného dodatku k této smlouvě.

3. Předmět smlouvy bude Objednateli Zhotovitelem předán na základě akceptačního protokolu, který bude podepsán odpovědnými zaměstnanci obou smluvních stran.

V. Místo plnění díla

1. Místem plnění díla je jak sídlo Objednatele, tak sídlo Zhotovitele.

VI. Práva a povinnosti smluvních stran

1. Objednatel je oprávněn průběh provádění díla kontrolovat. Zhotovitel je povinen předkládat Objednateli doklady a stanoviska, které získal v souvislosti s realizací díla.

2. Zhotovitel se zavazuje zachovávat mlčenlivost o skutečnostech a osobních údajích, s kterými přišel do styku při realizaci díla. Povinnost mlčenlivosti se nevztahuje na skutečnosti a informace, které:
a) mohou být zveřejněny bez porušení této smlouvy;
b) byly písemným souhlasem druhé smluvní strany uvolněny od těchto omezení;
c) jsou veřejně dostupné nebo byly zveřejněny jinak, než porušením či zanedbáním povinnosti jedné ze smluvních stran;
d) příjemce je zná zcela prokazatelně dříve, než je sdělí poskytující smluvní strana;
e) jsou vyžádány soudem, státním zastupitelstvím nebo věcně příslušným správním orgánem na základě zákona a jsou použity pouze k tomuto účelu.

3. Zhotovitel je povinen zavázat povinností mlčenlivosti všechny osoby, které se budou podílet na poskytování služeb dle této smlouvy včetně osob třetích stran, které mohou být přizvány po předchozím písemném souhlasu objednatele. Trvání mlčenlivosti není omezeno trváním této smlouvy

a trvá i po jejím zániku. Smluvní strany souhlasně prohlašují, že předmětem této smlouvy není přenos či zpracování osobních údajů. Nicméně poskytovatel se zavazuje v souvislosti s předmětem plnění této smlouvy, že pověření pracovníci, kteří i přesto přijdou do styku s osobními/citlivými údaji, učiní veškerá opatření, aby nedošlo k jejich neoprávněnému užití, změně, zcizení, ztrátě, zničení nebo neoprávněným přenosům.

4. Objednatel je povinen řádně a včas poskytovat Zhotoviteli při plnění jeho závazků z této smlouvy přiměřenou součinnost, zejména se vyjadřovat k průběhu realizace díla, k návrhům Zhotovitele, podávat Zhotoviteli potřebné informace a poskytovat nezbytné podklady, které má ve svém držení.

5. Objednatel odpovídá za správnost všech poskytnutých podkladů, jakož i za správnost poskytnutých informací. Objednatel se zavazuje, že veškeré podklady a informace bude poskytovat Zhotoviteli bez zbytečného odkladu po jejich vyžádání, bude-li to objektivně možné.

6. Jakékoli jednostranné právní jednání směřující k zániku účinnosti této smlouvy musí být učiněno v listinné podobě a musí být doručeno datovou zprávou, poštou (prostřednictvím držitele poštovní licence), kurýrem či osobně druhé smluvní straně, jinak se k němu nepřihlíží. Doručení musí být potvrzeno např. dodejkou, doručenkou nebo jiným obdobným dokladem, nevyplývá-li z této smlouvy jinak.

7. Obdrží-li Zhotovitel od Objednatele pokyn zřejmě nesprávný, upozorní Objednatele na jeho nevhodnost, přičemž jej splní pouze tehdy, bude-li Objednatel na provedení pokynu trvat a toto písemně Zhotoviteli oznámí.

VII. Záruka za dílo

1. Zhotovitel se zavazuje, že dílo bude mít vlastnosti stanovené v zadávací dokumentaci, ve specifikaci díla dle této smlouvy. V neposlední řadě se zhotovitel zavazuje, že dílo bude splňovat požadavky stanovené právními předpisy České republiky.

2. Smluvní strany si sjednávají záruční dobu 12 měsíců pro dílo dle fáze 1. a 36 měsíců pro dílo dle fáze 2.

3. Vyskytnou-li se v záruční době na předaném díle vady, musí tyto vady Objednatel reklamovat písemně u Zhotovitele na e-mail milan.kubat@alef.com. Písemná forma je podmínkou platnosti reklamace. Zhotovitel je pak povinen vady odstranit bez zbytečného odkladu nejpozději však do 3 pracovních dnů ode dne nahlášení vady, nedohodnou-li se strany písemně jinak.

4. V případě, že se jedná o vadu, kterou lze odstranit opravou, má Objednatel právo na bezplatné provedení opravy. V ostatním se uplatní ustanovení občanského zákoníku, přičemž pokud tento dává na výběr z více možností, právo volby má vždy Objednatel.

5. Vznikne-li objednateli v příčinné souvislosti s vadou díla škoda, je zhotovitel povinen objednateli škodu v plné výši nahradit.

VIII. Smluvní pokuty a sankce

1. V případě, že Zhotovitel bude v prodlení s termínem dokončení díla, zaplatí Objednateli smluvní pokutu ve výši 0,5% z celkové ceny díla včetně DPH za každý započatý den prodlení.

2. V případě, že Zhotovitel bude v prodlení s odstraněním vad v termínu dle této smlouvy, je Zhotovitel povinen Objednateli zaplatit smluvní pokutu ve výši 0,5 % z celkové ceny díla včetně DPH za každý započatý den prodlení.

3. V případě, že zhotovitel poruší povinnost mlčenlivosti sjednanou v čl. VI. Smlouvy, uhradí objednateli smluvní pokutu ve výši 10.000,- Kč za každý jednotlivý případ porušení povinnosti mlčenlivosti.

4. Zaplacením smluvní pokuty není dotčeno právo smluvní strany na náhradu škody vzniklé porušením smluvní povinnosti, které se smluvní pokuta týká.

5. Smluvní pokuty sjednané touto smlouvou jsou splatné do 14 dnů od jejich vyúčtování druhé smluvní straně.

IX. Další ustanovení

1. Veškeré věci, podklady a další doklady, které byly objednatelem zhotoviteli předány a nestaly se součástí díla, zůstávají ve vlastnictví objednatele, resp. objednatel zůstává osobou oprávněnou k jejich zpětnému převzetí. Zhotovitel je objednateli povinen tyto věci, podklady či ostatní doklady vrátit na výzvu objednatele, a to nejpozději ke dni řádného předání díla, s výjimkou těch, které prokazatelně a oprávněně spotřeboval k naplnění svých závazků z této smlouvy.

2. Dílo/jeho část se protokolárním předáním stává vlastnictvím objednatele, cena autorských práv je zahrnuta v ceně díla. Zhotovitel uděluje objednateli neomezený souhlas užít dílo, vyslovuje souhlas s bezplatnou reprodukcí, modifikací, dopracováním či prováděním jakýchkoliv změn díla způsobem dle vlastního uvážení a potřeb objednatele. Objednatel je oprávněn dílo užít, a to ke všem způsobům užití ve smyslu autorského zákona v neomezeném časovém, množstevním i územním rozsahu. Objednatel je oprávněn k pořízení trvalých rozmnoženin díla samostatně i ve spojení či v souboru s jinými autorskými či neautorskými díly, a to jakýmikoliv prostředky a v jakékoliv formě v libovolném počtu. Objednatel je neomezeně oprávněn k rozšiřování rozmnoženin díla. Objednatel je bez nároku zhotovitele na jakoukoliv odměnu, úplatu či náhradu škody apod. oprávněn s dílem nakládat. Objednatel má právo oprávnění dle tohoto ustanovení zcela nebo zčásti bez dalšího poskytnout třetí osobě, a to bez jakéhokoliv omezení, ať už místního, množstevního, časového či jiného a činit na něm změny bez omezení. K požadavku objednatele na modifikaci díla se zhotovitel zavazuje tomuto vyhovět.

3. Zhotovitel není oprávněn dílo dle této smlouvy poskytnout třetí osobě či využít jinak, než ve prospěch objednatele v souladu s touto smlouvou.

X. Závěrečná ujednání

1. Veškeré změny a doplňky smlouvy lze provést pouze formou písemných dodatků v listinné podobě podepsaných oběma smluvními stranami.

2. Pokud by kterékoli ustanovení v této smlouvě bylo nebo by se stalo neplatným nebo právně nevymahatelným, nebude to mít vliv na platnost a vymahatelnost ostatních ustanovení této smlouvy.

3. Tato smlouva je vyhotovena ve dvou stejnopisech, z nichž každá ze smluvních stran obdrží jedno vyhotovení.

4. Veškeré závazkové právní vztahy spojené s touto smlouvou se řídí příslušnými českými obecně závaznými právními předpisy, zejména pak zákonem č. 89/2012 Sb., občanský zákoník. Použití ustanovení § 557, § 1726, § 1728, § 1729, § 1740 odst. 3, § 1744, § 1757 odst. 2, 3, § 1770, § 1950, 2050, zák. č. 89/2012 Sb., občanského zákoníku, se vylučuje. Dále se vylučuje použití § 577 zák. č. 89/2012 Sb., občanský zákoník - určení množstevního, časového, územního nebo jiného rozsahu ve smlouvě je pevně určeno autonomní dohodou smluvních stran a soud není oprávněn do smlouvy jakkoli zasahovat.

5. Zhotovitel bere na vědomí a souhlasí, že tato smlouva bude v souladu se z. č. 340/2015 Sb., objednatelem uveřejněna v registru smluv.

6. Smluvní strany prohlašují, že je jim znám celý obsah smlouvy a že tuto smlouvu uzavřely na základě své svobodné a vážné vůle. Na důkaz této skutečnosti připojují svoje podpisy.

21 -05- 2019

V Olomouci dne 2019

V Praze dne 23. 4. 2019

[redacted]

Přílohy:

Příloha č. 1 – Požadavky a metodika na provedení jednotlivých fází implementace ZoKB ve FNOL a ISMS dle ISO 27001

Příloha č. 2 - Harmonogram implementace

Příloha č. 1

Požadavky a metodika na provedení jednotlivých fází implementace ZoKB ve FNOL a ISMS dle ISO 27001

1 Ustanovení a implementace ZoKB a ISMS dle ISO 27001

Požadujeme implementaci zákona o kybernetické bezpečnosti č. 181/2014 Sb. (ZoKB) a systému řízení bezpečnosti informací (dále jen ISMS) v rámci rozsahu a hranic systému řízení informační bezpečnosti v prostředí ICT organizace.

1.1 PDCA (plánuj, jednej, kontroluj, dělej) cyklus v rámci systému řízení bezpečnosti informací (dále jen ISMS)

PDCA cyklus zahrnuje následující fáze v rámci ISMS:

1.1.1 Plánuj (ustanovení ISMS, tj. pochopení požadavků na bezpečnost informací organizace a potřeb a stanovení politiky a cílů bezpečnosti informací)

1.1.2 Jednej (zavádění a provozování ISMS)

1.1.3 Kontroluj (monitorování a přezkoumání ISMS)

1.1.4 Dělej (udržování a zlepšování ISMS)

ISMS obsahuje následující aktivity / etapy projektu:

Fáze 1 (viz. Body realizace 2.1-2.5):

- Rozsah a hranice systému řízení informační bezpečnosti
  - vymezení z hlediska organizace - organizační rozsah dle organizační struktury, cílů
  - vymezení z hlediska řízených aktiv,
  - vymezení z hlediska informačních a komunikačních systémů
  - vymezení z hlediska fyzického rozsahu
  - doplnění / vyloučení

- Organizační role, odpovědnost a pravomoci v rámci ZoKB a ISMS
- Metodika hodnocení rizik
- Analýza rizik bezpečnosti informací (zahrnuje Identifikace a hodnocení aktiv)
- Návrh plánu ošetření rizik /zvládání rizik a Prohlášení o aplikovatelnosti (formalizace závěrů – vstup pro Risk registr, Management commitment, formalizace řešení rizik a přístup vedení pro řízení rizik)

Fáze 2 (viz. Body realizace 2.6-2.11):

- Bezpečnostní politika a Bezpečnostní a provozní dokumentace, návrh ISMS - organizace, role, odpovědnost
- Plán bezpečnostního vědomí zaměstnanců (školení, informovanost, odborná způsobilost)
- Interní audity a Přezkoumání ISMS
- Proces kontinuálního zlepšování

- Harmonizace a podpora přípravy organizace v dalších činnostech

2 Realizace implementace

2.1 Rozsah a hranice systému řízení informační bezpečnosti

Cílem fáze je:

- vymezení z hlediska organizace - organizační rozsah dle organizační struktury, cílů
- vymezení z hlediska řízených aktiv,
- vymezení z hlediska informačních a komunikačních systémů
- vymezení z hlediska fyzického rozsahu
- doplnění / vyloučení

2.2 Organizační role, odpovědnost a pravomoci v rámci ZoKB a ISMS

Cílem fáze je definovat organizační role, odpovědnost a pravomoci v rámci požadavků Zákona o kybernetické bezpečnosti (ZoKB) a vyhlášky 82/2018 Sb. a ISMS dle ISO 27001.

Popis provedení

V této fázi budou provedeny následující úkony, které jsou předepsány ZoKB, resp. VoKB č. 82/2018 Sb. a normou ČSN ISO/IEC 27001:2014 či jsou důležité pro realizaci zavedení ISMS:

Vrcholové vedení zajistí, že odpovědnosti a pravomoci týkající se rolí důležitých pro bezpečnost informací jsou přiděleny a komunikovány.

Vrcholové vedení přidělí odpovědnost a pravomoci pro:

a) zajištění, aby systém řízení bezpečnosti informací odpovídal požadavkům ZoKB a ISMS,
b) podávání zpráv o výkonu systému řízení bezpečnosti informací na vrcholový management.

Identifikace změn v organizační struktuře formou interview se zástupci FNOL, jež mohou mít dopad na součinnost ze strany FNOL a na implementaci ISMS v FNOL

Výstupy fáze

Ustanovení klíčových rolí, jejich odpovědností a pravomocí ve FNOL, které se podílejí na bezpečném provozu služeb a systému řízení bezpečnosti informací FNOL. Částečně již FNOL řeší ustanovením a zahájením práce Výboru KB.

2.3 Metodika hodnocení rizik

Cílem fáze je stanovit metodiku pro analýzu rizik informační bezpečnosti dle ISO 27001 a VoKB č. 82/2018 Sb.

Popis provedení

V této fázi budou provedeny následující úkony, které jsou předepsány normou ČSN ISO/IEC 27001:2014 a VoKB č. 82/2018 Sb. či jsou důležité pro realizaci zavedení ISMS:

- provedení výběru informačních hrozeb a zranitelností pro Analýzu rizik dle ISO 27000 a VoKB č 82/2018 Sb.
- stanovení pravidla pro hodnocení rizik souvisejících s dodavateli (následně bude součástí politiky řízení dodavatelů)
- navržení Metodiky pro identifikaci a hodnocení rizik bezpečnosti informací;
- projednání a předání Metodiky k posouzení ze strany FNOL;
- zapracování připomínek k Metodice.

Výstupy fáze

- Metodika pro hodnocení rizik bezpečnosti informací, která stanovuje postupy a kritéria pro identifikaci (formulaci) a hodnocení hrozeb, zranitelností a dopadů a stanovuje výpočet rizik bezpečnosti informací. Metodika je postavena na principech ISO/IEC 27000 a vyhlášky 82/2018 Sb. Hodnotící kritéria zahrnují hlediska zachování důvěrnosti (klasifikace), integrity a dostupnosti informačních aktiv.

2.4 Analýza rizik bezpečnosti informací

Cílem fáze je určit a vyhodnotit rizika, která hrozí informačním aktivům FNOL.

Popis provedení

V této fázi budou provedeny následující úkony, které jsou předepsány normou ČSN ISO/IEC 27001:2014 a VoKB č. 82/2018 Sb. či jsou důležité pro realizaci zavedení ISMS:

- provedení výběru respondentů pro provedení analýzy rizik;
- provedení interview - rozhovorů k analýze rizik;
- hodnocení hrozeb, zranitelností, stávající bezpečnostní opatření a návrhy dodatečných opatření primárních aktiv;
- hodnocení hrozeb, zranitelností, stávající bezpečnostní opatření a návrhy dodatečných opatření podpůrných aktiv;
- provedení zpracování dat z interview;
- vytvoření, průběžné posouzení a reportování registru rizik;
- navržení úrovní pro akceptaci rizik;
- stanovení vlastníků rizik;
- zpracování Zprávy z analýzy rizik;
- projednání a předání Zprávy k posouzení ze strany FNOL;
- zapracování připomínek ke Zprávě;
- zpracování a předání finální verze Zprávy.

Analýza rizik bude zahrnovat systémová/ procesní rizika a technologická rizika.

Výstupy fáze

- Zpráva o hodnocení rizik bezpečnosti informací v FNOL – obsahuje následující části:
  - přehled aktiv včetně určení jejich hodnot z hlediska ISMS a VoKB č. 82/2018 Sb. a stanovení vlastníků;
  - výčet hrozeb a zranitelností, která na aktiva (skupiny aktiv) působí;

- stanovení a vyhodnocení rizik pro jednotlivá aktiva a stanovení vlastníků rizik;
- návrh úrovní pro akceptaci rizik;
- návrh vlastnictví rizik;
- manažerské shrnutí a interpretace výsledků analýzy rizik.

2.5 Návrh plánu ošetření rizik /zvládání rizik a Prohlášení o aplikovatelnosti

Cílem fáze je formalizace závěrů z Analýzy rizik jako vstup pro Risk registr a zároveň definování návrhu plánu ošetření / zvládání rizik, jež zahrnuje výčet cílů opatření jak ošetřit rizika zjištěná v rámci provedené analýzy rizik a seznamu zbytkových rizik k akceptaci.
Součástí této fáze je také připravení Prohlášení o aplikovatelnosti.

Popis provedení
V této fázi budou provedeny následující úkony, které jsou předepsány normou ČSN ISO/IEC 27001:2014 a VoKB č. 82/2018 Sb. či jsou důležité pro realizaci zavedení ISMS:

- formalizace závěrů jako vstup pro Risk registr z Analýzy rizik,
- navržení a odsouhlasení způsobu zvládání rizik;
- provedení rozhovorů ke zpracování Plánu ošetření rizik s vlastníky rizik:
    - identifikace stávajících bezpečnostních opatření,
    - navržení dodatečných bezpečnostních opatření k redukci rizik,
    - expertní odhad účinnosti identifikovaných opatření.
    - návrh prioritizace redukce rizik
- zpracování Plánu ošetření/ zvládání rizik;
- projednání a předání Plánu ošetření/ zvládání rizik k posouzení ze strany FNOL;
- zapracování připomínek k Plánu ošetření / zvládání rizik;
- zpracování a předání finální verze Plánu ošetření / zvládání rizik a seznamu zbytkových rizik ke schválení v FNOL.
- projednání a schválení návrhu Plánu ošetření / zvládání rizik a seznamu zbytkových rizik FNOL.
- příprava vhodné struktury Prohlášení o aplikovatelnosti (PoA) dle VoKB a ISO 27001 / kontrolní seznam (checklist) bezpečnostních opatření;

Předpoklad

- Prohlášení o aplikovatelnosti (PoA) bude obsahovat přehled bezpečnostních opatření celkově pro celou organizaci, bez členění způsobu plnění v jednotlivých organizačních jednotkách.

Výstupy fáze

- Návrh plánu ošetření rizik/ zvládání rizik – popisuje sadu bezpečnostních opatření pro redukci identifikovaných rizik k následné implementaci, včetně jejich prioritizace
- Obsahem tohoto dokumentu budou následující údaje:
    - jednotlivá opatření vybraná dle ČSN ISO/IEC 27001:2014 a VoKB č. 82/2018 Sb.;
    - případná další opatření;
    - expertní odhad účinnosti opatření k redukci rizika.
- Formalizace závěrů jako vstup pro Risk registr z Analýzy rizik
- Návrh seznamu zbytkových rizik k akceptaci včetně zdůvodnění.

- Prohlášení o aplikovatelnosti – obsahuje souhrnný přehled opatření, která jsou aplikována v FNOL a případné důvody pro neaplikování nerelevantních opatření. Prohlášení o aplikovatelnosti bude reflektovat ČSN ISO/IEC 27001:2014 a požadavky VoKB č. 82/2018 Sb.

2.6 Bezpečnostní politika

Cílem fáze je identifikace stávající existující dokumentace, dokumentování a formalizace procesu řízení bezpečnosti informací a rizik informací (Information Risk Management – IRM) v FNOL, vypracování Bezpečnostní politiky v oblasti systému řízení bezpečnosti informací v souladu s ČSN ISO/IEC 27001:2014 a podle požadavků Vyhlášky o kybernetické bezpečnosti č.82/2018 Sb. (VoKB) pro následné začlenění do stávajícího systému dokumentace FNOL.

Popis provedení

V této fázi bude provedena revize a doplnění stávající dokumentace a bude zpracována jednotná Bezpečnostní politika v oblasti systému řízení bezpečnosti informací, která bude obsahovat kapitoly dle požadavků normy ČSN ISO/IEC 27001:2014 a oblasti uvedené v příloze č. 5 (čl. 1. 1. – 1.23) VoKB č. 82/2018 Sb. Bude tedy stanovovat systémové požadavky na ISMS v šíři celé organizační struktury.

Bezpečnostní politika bude zpracována tak, aby obsahovala hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací FNOL. Tato fáze bude obsahovat kroky:

- Návrh vhodné struktury Bezpečnostní politiky splňující požadavky VoKB č. 82/2018 Sb., normy ISO 27001 pro následné začlenění do stávajícího systému dokumentace FNOL.
- Odsouhlasení návrhu struktury Bezpečnostní politiky odpovědnými osobami.
- Návrh Bezpečnostní politiky:
    - provedení výběru respondentů k návrhu Bezpečnostní politiky v jednotlivých oblastech,
    - návrh Bezpečnostní politiky ve všech oblastech,
    - provedení interview – rozhovorů k návrhu Bezpečnostní politiky v jednotlivých oblastech,
    - přizpůsobení Bezpečnostní politiky a připomínkování návrhu bezpečnostní politiky,
    - zapracování připomínek k Bezpečnostní politice,
    - zpracování konečného návrhu Bezpečnostní politiky,

Výstupy fáze

- Zavedení a formalizace procesu systému řízení bezpečnosti informací a řízení rizik informací
- Bezpečnostní politika v oblasti systému řízení bezpečnosti informací – dokument obsahující hlavní zásady, cíle, potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací FNOL, definující specifické požadavky a postupy pro řízení systému informační a kybernetické bezpečnosti a naplnění bezpečnostních a regulatorních požadavků.

2.7 Plán rozvoje bezpečnostního povědomí

Cílem fáze je vypracovaní návrhu Plánu rozvoje bezpečnostního povědomí ve struktuře dle požadavků vyhlášky č. 82/2018 Sb., který bude obsahovat koncepci tvorby a budování bezpečnostního povědomí subjektů účastnících se správy, provozu a užívání informací a informačních systémů v FNOL.

Popis provedení

V rámci fáze budou provedeny následující činnosti:

- Vytvoření koncepce tvorby a budování bezpečnostního povědomí zaměstnanců a dodavatelů FNOL - subjektů účastnících se správy, provozu a užívání informací a informačních systémů v FNOL.
- Definování skupin (kategorií) cílových skupin zvyšování bezpečnostního povědomí a odsouhlasení cílových skupin (např. běžný uživatel, administrátor a operátor ICT, bezpečnostní management, dodavatel).
- Návrh způsobů poučení výše uvedených cílových skupin zahrnující:
    - přímou edukaci (školení, workshopy, kurzy, ...),
    - nepřímou edukaci (e-learning, webináře, ...),
    - další formy zvyšování bezpečnostního povědomí (např. vzdělávací kampaně, plakáty, newslettery, semináře, ...)
- Definice požadavků na vstupní, periodická a mimořádná školení a návrh jejich obsahu (formou krátkého popisu) a termínů (periodicity) poučení výše uvedených skupin
- Návrh způsobu ověření rozvoje bezpečnostního povědomí – forma a způsob ověření bezpečnostního povědomí např. praktikami sociálního inženýrství, návrhem metrik kvality a účinnosti vzdělávacích programů

Výstupy fáze

- Dokument obsahující koncepci tvorby a budování bezpečnostního povědomí zaměstnanců FNOL.
- Plán rozvoje bezpečnostního povědomí
- Popis obsahu a určení periodicity poučení zaměstnanců
- Návrh způsobu poučení nových zaměstnanců
- Návrh způsobu ověření rozvoje bezpečnostního povědomí

2.8 Interní audity ISMS

2.8.1 Plán vnitřních auditů

Cílem fáze je vytvořit návrh systému interního auditu ISMS, zpracovat program auditů ISMS a vzor plánu auditu ISMS FNOL, které budou sloužit k posouzení míry zavedení a efektivnosti procesů a opatření ISMS FNOL.

Popis provedení

V této fázi budou provedeny následující úkony, které jsou předepsány ZoKB i normou ČSN ISO/IEC 27001:2014 a jsou důležité pro realizaci zavedení ISMS:

- Zpracování metodiky řízení interních auditů ISMS
- Projednání způsobu provádění interních auditů ISMS, upřesnění auditovaných oblastí a procesů ISMS, jmenování auditorů;
- Zpracování a projednání Programu interního auditu ISMS, který bude obsahovat:
    - Bezpečnostní audity,
    - manuální či automatizované kontroly technické shody,
    - penetrační testy a analýza zranitelností,
    - audity za použití nástrojů sloužících pro kontrolu provozních systémů.
- Zpracování vzoru Plánu interního auditu ISMS;

Výstupy fáze

- Program interního auditu ISMS – dokument popisující auditované oblasti ISMS, zdroje, požadavky na součinnost a perioda provedení interních auditů ISMS.
- Plán interního auditu ISMS – dokument upřesňující provedení konkrétního interního auditu ISMS.
- Metodika řízení interních auditů ISMS

2.9 Přezkoumání ISMS

2.9.1 Pravidla a postupy pro přezkoumání ISMS

Cílem fáze je vytvořit systém přezkoumání systému ISMS FNOL vedením společnosti.

Popis provedení

V této fázi budou provedeny následující úkony tvořící systém přezkoumání systému ISMS FNOL vedením společnosti dle ZoKB a požadavků ISO 27001:

- Vypracování metodiky přezkoumání systému řízení bezpečnosti informací, stanovení vstupů a způsobu sběru dat pro přezkoumání systému řízení bezpečnosti informací
- Návrh, konzultace a zpracování vzoru přezkoumání systému řízení bezpečnosti informací, obsahující strukturu a obsah přezkoumání (s uvedením požadovaných kapitol a stručného popisu obsahu kapitol)
- Zapracování připomínek k dodaným výstupům

Výstupy fáze

- Metodika přezkoumání systému řízení bezpečnosti informací
- Specifikace vstupů pro přezkoumání
- Struktura přezkoumání systému řízení bezpečnosti informací

2.10 Proces a kontinuální zlepšování

Cílem fáze je vytvořit Proces kontinuálního zlepšování, pravidla a postupy pro neustálé zlepšování včetně rolí a odpovědností pro výkon činností v rámci tohoto procesu na základě tzv. Demingova cyklu (PDCA) neustálého zlepšování. Zlepšování procesů má za cíl maximalizaci potenciálu organizace a je spojen s minimalizací entropie (míra neurčitosti procesu). Cílem je neustále zlepšovat servis a procesy. Tato metoda hledá „inkrementální" zlepšování v čase nebo „průlomové" zlepšení. Vykonávané procesy jsou neustále zkoumány a zlepšovány za účelem zlepšení jejich efektivnosti, účinnosti a flexibility.

Popis provedení

V této fázi budou provedeny následující úkony, které jsou předepsány ZoKB i normou ČSN ISO/IEC 27001:2014 a jsou důležité pro realizaci zavedení ISMS:

a) zavedení systému a procesu kontinuálního zlepšování systému řízení bezpečnosti informací FNOL v souladu s požadavky normy pro řízení systému informační bezpečnosti a řízení kybernetické bezpečnosti
b) přezkoumávání systému řízení bezpečnosti informací FNOL

Výstupy fáze

Dokument definující proces kontinuálního zlepšování, pravidla a postupy pro neustálé zlepšování včetně rolí a odpovědností pro výkon činností v rámci tohoto procesu.

2.11 Harmonizace a podpora přípravy organizace v dalších činnostech

Cílem fáze je poskytnout podporu a konzultace FNOL pro zajištění dalších činností a naplňování požadavků v oblasti ZoKB a ISMS, případné revize a další doplnění, aktualizace dle požadavků a následnou harmonizaci a součinnost v přípravě pro další rozvoj a naplňování požadavků FNOL,

Popis provedení

Konzultace a projednání požadavků organizace pro zajištění dalších činností a naplňování požadavků v oblasti ZoKB a ISMS, či v jiné oblasti, kterou organizace potřebuje řešit nebo integrovat, ověřit a harmonizovat do současného prostředí FNOL.

Výstupy fáze

Konkrétní doporučení a výstupy na požadavky FNOL, které budou nezbytné pro další rozvoj činností a služeb, projednání se zástupci FNOL. Posledním výstupem a dokončením splnění fáze 2. se rozumí vypořádání závěrů externího auditu zhotovitelem, pokud objednatel tohoto využije.

Příloha č. 2

Harmonogram implementace

Body fáze I.	Termín realizace
Rozsah a hranice systému řízení informační bezpečnosti	T0 + 0,5 měsíce
Organizační role, odpovědnost a pravomoci v rámci ZoKB a ISMS	T1 + 0,5 měsíc
Metodika hodnocení rizik	T2 + 0,5 měsíc
Analýza rizik bezpečnosti informací (zahrnuje Identifikace a hodnocení aktiv)	T3 + 1,5 měsíce
Návrh plánu ošetření rizik /zvládání rizik a Prohlášení o aplikovatelnosti	T4 + 2 měsíce

T0 – termín T0 bude upřesněn po zahajovací schůzce dle kapacit Zadavatele

Body fáze II.	Termín realizace
Bezpečnostní politika a Bezpečnostní a provozní dokumentace, návrh ISMS - organizace, role, odpovědnost	T5 + 7 měsíců
Plán bezpečnostního vědomí zaměstnanců (školení, informovanost, odborná způsobilost)	T6 + 1 měsíc
Interní audity a Přezkoumání ISMS	T7 + 1 měsíc
Proces kontinuálního zlepšování	T8 + 1 měsíc
Harmonizace a podpora přípravy organizace v dalších činnostech	T9 + 0,5 měsíce