SMLOUVA O POSKYTNUTÍ SLUŽBY

Číslo smlouvy LIS 2024_2_083

Uzavřená dle ustanovení Zákona č. 89/2012 Sb, Občanského zákoníku.

1. **Objednatel:** **Liberecká IS, a.s.**
   Se sídlem: **Mrštíkova 850/3, 460 07, Liberec III - Jeřáb**
   Zastoupený: **Ing. Jaroslavem Burešem, MBA, předsedou představenstva**
   IČ: **25450131**
   DIČ: **CZ25450131**
   Bank. spojení: ČSOB a.s., číslo účtu: 267710810/0300
   Společnost je zapsána v Obchodním rejstříku u Krajského soudu v Ústí nad Labem, oddíl B, vložka 1429.
   (dále jen Objednatel)

2. **Poskytovatel:** **Next Generation Security Solutions s.r.o.**
   Se sídlem: **U Uranie 954/18, 170 00 Praha 7**
   Zastoupený: **Mgr. Ondřejem Dedkem, jednatelem**
   IČ: **06291031**
   DIČ: **CZ06291031**
   Bank. spojení: ČSOB a.s., číslo účtu: 301 607 295/0300
   Společnost je zapsána v Obchodním rejstříku u Městského soudu v Praze, oddíl C, vložka 279627
   (dále jen Poskytovatel)

(oba též společně jako smluvní strany)

PREAMBULE SMLOUVY

Podkladem pro uzavření této Smlouvy o dílo (dále také „Smlouva“) je nabídka Dodavatele podaná pro veřejnou zakázku „Zavedení systému řízení bezpečnosti informací a báze znalostí v oblasti KB 16/2024" (dále jen „Veřejná zakázka“) zadávanou Objednatelem dle vlastní interní směrnice 3.1 2017 02 Pravidla pro výběr dodavatelů a zadávání zakázek a Pokynu vlastníka komponent 1.1, 1.2 a 4.4 pro příjemce finanční podpory NPO. Tato Smlouva byla uzavřena v souladu se všemi podmínkami uvedenými v zadávací dokumentaci.

I. PŘEDMĚT SMLOUVY

1. Předmětem této smlouvy je služba

   Zavedení systému řízení bezpečnosti informací (dále SŘBI) a báze znalostí v oblasti kybernetické bezpečnosti v souladu s novelizovaným Zákonem o kybernetické bezpečnosti (dále ZKB) a Směrnicí evropského parlamentu NIS 2 (dále NIS 2), a to dle podmínek uvedených v bodech 1. a) – 1. d) tohoto článku.

   V rámci poskytnuté služby budou pokryty klíčové oblasti kybernetické bezpečnosti Objednatele, které budou zajištěny prostřednictvím implementace (vytvoření a zavedení) katalogů bezpečnostních politik, pravidel, procesů a služeb začleněných do okolních procesů zadavatele, dále bude podpořena strategie směřování Objednatele, budou stanoveny cíle SŘBI a popsány potřeby pro řízení zdrojů. Realizace předmětu smlouvy musí naplnit následující podmínky:

a) zavedení SŘBI v rámci realizace této smlouvy bude provedeno dle požadavků uvedených v návrzích novely ZKB a navazujících vyhlášek, které byly předloženy Poslanecké sněmovně ČR (dále PS ČR) ke schválení.

b) Pokud bude novela ZKB a navazující vyhlášky schválená PS ČR k dispozici v době realizace této zakázky, bude zavedený systém SŘBI plně v souladu se schváleným zněním této legislativy.

c) Zadavatel si uvědomuje, že pokud schválená novela ZKB a navazujících vyhlášek nebudou k dispozici v době realizace této zakázky a následně dojde ke změnám návrhů nové legislativy v průběhu schvalovacího řízení, bude nucen následně upravit zavedený SŘBI dle těchto změn. Tyto následné úpravy nejsou předmětem této zakázky.

d) Liberecká IS, a.s. se na zavedení nové legislativy v oblasti SŘBI již připravuje a v rámci této přípravy již:

1. Definovala aktiva společnosti
2. Definovala hrozby působící na aktiva společnosti
3. Provedla hodnocení rizik vyplývajících z definovaných hrozeb
4. Provedla návrh opatření k eliminaci definovaných rizik a stanovila „Strategii rozvoje služeb technické bezpečnosti pro Informační systém statutárního města Liberec“

Název položky	Počty	Základní popis položky
Primární aktiva	14	Aplikační, systémové, telekomunikační služby, datové přenosy, bezpečnost IT, nákupy, lidské zdroje, materiální a finanční zdroje, řízení firmy, administrativa
Podpůrná aktiva	65	Rozpad z primárních aktiv, aplikace, dodavatelé, infrastruktura, úložiště atd.
Počet působících hrozeb celkem	44	Všechny typy působících hrozeb, jež jsou přiřazeny v rámci hodnocení rizik
Počet definovaných opatření k realizaci	27	Procesy, nákupy, zabezpečení atd.

Tyto podstatné aktivity pro zavedení SŘBI jsou tedy v prostředí zadavatele realizovány a proto zadavatel požaduje, aby zavedení SŘBI dle tohoto poptávkového řízení navazovalo na výše uvedené aktivity a aby účastník existenci těchto podstatných aktivit zohlednil v nabídkové ceně.

2. Zavedení SŘBI a báze znalostí v oblasti kybernetické bezpečnosti dle tohoto poptávkového řízení bude zahrnovat návrh postupů a jejich zdokumentování především v oblastech:
   1. Řízení rizik
   2. Bezpečnostní politika
   3. Organizační bezpečnost
   4. Řízení dodavatelů
   5. Řízení aktiv
   6. Bezpečnost lidských zdrojů
   7. Řízení provozu a komunikací
   8. Řízení přístupů osob
   9. Akvizice, vývoj, údržba / Řízení změn
   10. Zvládání kybernetických bezpečnostních událostí a incidentů (dále také “KBU” a “KBI”)
   11. Řízení kontinuity činností
   12. Interní audit kybernetické bezpečnosti
3. Samotné zavedení systému řízení bezpečnosti informací pro pokrytí požadavků kybernetické bezpečnosti bude realizováno v rámci tří na sebe navazujících etap:
   1. Etapa 0 – Vypracování cílového konceptu
   2. Etapa I. – Implementace vybraných bezpečnostních opatření
   3. Etapa II. – Interní audit kybernetické bezpečnosti
4. Detailní popis služby je uveden v příloze č. 1 této smlouvy.
5. Objednatel se zavazuje řádně odvedenou službu převzít a zaplatit za ni dohodnutou odměnu.

6. **Objednatel nepožaduje zavedení systému bezpečnosti informací dle normy ISO 27001, protože tuto normu již ve svém prostředí implementovanou má!**
7. Jako součást plnění dle článku I., odst. 1. této smlouvy Poskytovatel pro Objednatele vypracuje do 21 dnů od účinnosti této smlouvy cílový koncept a předloží jej Objednateli k odsouhlasení. Cílový koncept bude minimálně obsahovat:
   a) Návrhy na úpravu časového harmonogramu jednotlivých etap plnění předmětu smlouvy dle přílohy č. 2 této smlouvy (dále harmonogram).
   b) Popisnou část, kde budou jednotlivé kroky a činnosti, případně vazby dle harmonogramu popsány;
   c) Věcnou specifikaci jednotlivých etap plnění předmětu smlouvy dle harmonogramu, konkrétní plán prací a činností v jednotlivých etapách, které je nutné provést k úspěšné realizaci předmětu plnění této smlouvy. Obsahem bude také definice rolí jednotlivých zástupců Poskytovatele i Objednatele, podrobný postup dosažení jednotlivých etap, specifikace potřebných vstupů, milníky jednotlivých etap, testovací scénáře apod.;
   d) Cílový koncept musí respektovat a zahrnovat všechny procesy, funkcionality, specifikace a požadavky stanovené v příloze č. 1 této smlouvy;
   e) Obsah cílového konceptu musí být vzájemně prokazatelně odsouhlasen oběma smluvními stranami. Akceptace cílového konceptu Objednatelem je nezbytnou podmínkou pro zahájení dalších realizačních prací na plnění předmětu smlouvy.

II. TERMÍN PŘEDÁNÍ SLUŽBY

1. Poskytovatel poskytne službu uvedenou v článku I. této smlouvy a detailně popsanou v příloze č. 1 této smlouvy nejpozději do 31. 8. 2025.
2. Služba bude předána na základě akceptačního protokolu podepsaného odpovědnou osobou za stranu Objednatele i Poskytovatele.

III. ODMĚNA A PLATEBNÍ PODMÍNKY

1. Za úplnou službu poskytnutou Poskytovatelem dle článku I. odstavec 1 této smlouvy zaplatí Objednatel odměnu celkem ve výši 1 299 400,- Kč bez DPH. K ceně bude připočítána DPH v platném znění ve výši 272 874,- Kč. Cena celkem 1 572 274,- Kč včetně DPH.
2. Na základě akceptačního protokolu je Poskytovatel oprávněn vystavit fakturu a zaslat ji elektronicky na e-mailovou adresu eko@is.liberec.cz. Faktura musí obsahovat všechny náležitosti daňového dokladu a přílohou musí být podepsaný akceptační protokol. Na faktuře bude uvedeno číslo smlouvy Objednatele. Dnem zdanitelného plnění bude datum podpisu akceptačního protokolu.
3. Splatnost faktury je 30 kalendářních dní ode dne jejího doručení Objednateli. Za den úhrady ceny je považován den, kdy příslušná částka bude připsána na účet Poskytovatele.

IV. ODPOVĚDNÉ OSOBY A ZPŮSOBY KOMUNIKACE

1. Smluvní strany si do 5 dnů od podpisu této smlouvy sdělí kontaktní údaje odpovědných osob nezbytně nutných pro řádné splnění předmětu této smlouvy.
2. Veškerá komunikace probíhá zásadně v českém jazyce.
3. Objednatel požaduje, aby pracovní schůzky probíhaly prioritně v sídle Objednatele, a to za osobní účasti dotčených členů týmu Poskytovatele. Minimální frekvence osobních schůzek bude 1x za 14 dnů.
4. Způsob předávání dokumentů potřebných k plnění předmětu smlouvy:
   - ✓ Dokumenty budou předávány přednostně v el. podobě, a to prostřednictvím bezpečného úložiště zajištěného Objednatelem,
   - ✓ Úložiště pro dokumenty bude v datovém centru Objednatele. Zástupci Poskytovatele obdrží přístupová povolení k tomuto úložišti,
   - ✓ Přístup k úložišti bude povolen pouze pro autorizovaná zařízení členů týmu Poskytovatele,
   - ✓ Předávané dokumenty budou opatřeny přístupovým heslem.

V. ROZSAH ODPOVĚDNOSTI ZA ŠKODU, SANKCE

1. Plnění smlouvy bude členěno na dílčí termíny dle harmonogramu uvedeného v příloze č. 2 této smlouvy. V těchto dílčích termínech bude Poskytovatel povinen předat Objednateli příslušné dokumenty uvedené v předmětu smlouvy, resp. v příloze č. 1 této smlouvy.

1. Poskytovatel je zodpovědný za vady, které vzniknou jeho zaviněním.
2. Poskytovatel není v prodlení, je-li jeho prodlení zapříčiněno prodlením na straně Objednatele.
3. Nedodrží-li Objednatel termín splatnosti, je Poskytovatel oprávněn požadovat smluvní úrok z prodlení ve výši 0,1 % z celkové nezaplacené částky za každý kalendářní den prodlení.
4. Nedodrží-li Poskytovatel dílčí termín harmonogramu dle přílohy č. 2 této smlouvy, je Objednatel oprávněn požadovat smluvní pokutu ve výši 1000,- Kč za každý kalendářní den prodlení oproti stanovenému dílčímu termínu.
5. Nedodrží-li Poskytovatel dílčí termín harmonogramu dle přílohy č. 2 této smlouvy po dobu delší než 30 kalendářních dnů, je Objednatel oprávněn okamžitě odstoupit od smlouvy.
6. Nedodrží-li Poskytovatel konečný termín úplného předání služby, je Objednatel oprávněn požadovat smluvní pokutu ve výši 0,1 % z celkového plnění dle čl. III. odst. 1. smlouvy za každý kalendářní den prodlení. Maximální smluvní pokuta je rovna ceně za celkové plnění předmětu smlouvy.
7. Uplatnění smluvní pokuty nezbavuje smluvní strany práva na náhradu škody způsobené porušením smlouvy druhou stranou. Odpovědnost za škody se řídí obecně závaznými právními předpisy České republiky.

VI. DOBA TRVÁNÍ A PLATNOST SMLOUVY

Platnost této smlouvy se sjednává na dobu určitou, a to do 31. 8. 2025.

VII. DŮVĚRNÉ INFORMACE

1. Pokud nebude dohodnuto jinak, každá ze zúčastněných stran se zavazuje, že utají před třetími stranami a osobami důvěrné informace a know-how, které získá na základě stávající smlouvy od strany druhé, zejména informace a skutečnosti tvořící obchodní, hospodářské nebo jiné utajované skutečnosti. Smluvní strany za důvěrné a utajované považují vedle informací výslovně označených jako důvěrné nebo tajné také takové informace, které nejsou všeobecně a veřejně známé, běžně dostupné, a které mohou svým zveřejněním způsobit škodlivý následek pro kteroukoli smluvní stranu.
2. Smluvní strany zaváží své zaměstnance, kteří přijdou do styku s důvěrnými informacemi ve smyslu tohoto odstavce k takovému zacházení s těmito informacemi, aby nedošlo k porušení závazků dle této smlouvy.

VIII. ZÁVĚREČNÁ USTANOVENÍ

1. Tato smlouva představuje úplnou dohodu mezi smluvními stranami. Tato smlouva může být měněna pouze formou písemných dodatků odsouhlasených oběma smluvními stranami. Návrhy dodatků je oprávněna předkládat každá ze smluvních stran.
2. Práva a povinnosti smluvních stran se řídí ustanoveními této smlouvy a ustanoveními občanského zákoníku. V případě konfliktu mají přednost ustanovení této smlouvy, pokud nejsou v rozporu s kogentními ustanoveními občanského zákoníku.
3. Smluvní strany se tímto zavazují, že si vzájemně poskytnou veškerou součinnost a vyvinou maximální možné úsilí potřebné k realizaci a naplnění této smlouvy. Smluvní strany jsou povinny si vzájemně sdělovat informace, které mohou mít vliv na plnění závazků vyplývajících z této smlouvy.
4. Otázky touto smlouvou výslovně neupravené budou posuzovány podle právních předpisů České republiky, zejména podle ustanovení Občanského zákoníku.
5. Smluvní strany se dohodly, že řešením veškerých případných sporů, jež by z této smlouvy nebo v souvislosti s ní vznikly, bude pověřen příslušný obecný soud v místě sídla Objednatele.
6. Smluvní strany jsou oprávněny zveřejnit veškerý obsah této smlouvy, budou-li o to požádány dle zákona č. 106/99 Sb.

7. Smluvní strany berou na vědomí, že tato smlouva bude zveřejněna v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).
8. Smlouva nabývá účinnosti dnem uveřejnění v registru smluv v souladu s § 6 odst. 1 zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).
9. Smluvní strany berou na vědomí, že plnění podle této smlouvy poskytnutá před její účinností jsou plnění bez právního důvodu a strana, která by plnila před účinností této smlouvy, nese veškerou odpovědnost za případné škody takového plnění bez právního důvodu, a to i v případě, že druhá strana takové plnění přijme a potvrdí jeho přijetí.
10. Tato smlouva je vyhotovena ve dvou stejnopisech, z nichž každá ze smluvních stran si ponechá jedno vyhotovení.
11. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami.
12. Nedílnou součástí smlouvy je příloha č. 1 Specifikace služby.
13. Nedílnou součástí smlouvy je příloha č. 2 Harmonogram plnění smlouvy.

V Praze dne (dle el. podpisu):
Za Poskytovatele:

V Liberci dne (dle el. podpisu):
Za Objednatele:

.....
Mgr. Ondřej Dedek
jednatel

.....
Ing. Jaroslav Bureš, MBA
předseda představenstva

Specifikace služby „Zavedení systému řízení bezpečnosti informací a báze znalostí v oblasti KB" v Liberecké IS, a.s.

Seznam zkratek:

SŘBI	systém řízení bezpečnosti informací
PoA	prohlášení o aplikovatelnosti
BPMN	modelovací jazyk (Business Process Model and Notation)
ZKB	zákon o kybernetické bezpečnosti
VKB	vyhláška o kybernetické bezpečnosti
KB	kybernetická bezpečnost
ISMS	integrovaný systém managementu společnosti
IS / KS	informační / komunikační systém
ZZOÚ	zákon o zpracování osobních údajů
SLA	dohoda o úrovni poskytovaných služeb
KBU	kybernetická bezpečnostní událost
KBI	kybernetický bezpečnostní incident
OWASP	doporučení k zabezpečení webových aplikací
SDP	Session Description Protocol
SAST	Static application security testing
DAST	Dynamic Application Security Testing
IAST	Interactive Application Security Testing
RASP	Runtime application self-protection

Poskytnutá služba zabezpečí:

Zavedení systému řízení bezpečnosti informací (dále SŘBI) a báze znalostí v oblasti kybernetické bezpečnosti v souladu s novelizovaným Zákonem o kybernetické bezpečnosti (dále ZKB) a Směrnicí evropského parlamentu NIS 2 (dále NIS 2), a to dle dále uvedených podmínek.

V rámci poskytnuté služby budou pokryty klíčové oblasti kybernetické bezpečnosti Objednatele, které budou zajištěny prostřednictvím implementace (vytvoření a zavedení) katalogů bezpečnostních politik, pravidel, procesů a služeb začleněných do okolních procesů zadavatele, dále bude podpořena strategie směřování Objednatele, budou stanoveny cíle SŘBI a popsány potřeby pro řízení zdrojů. Realizace předmětu smlouvy musí naplnit následující podmínky:

a) zavedení SŘBI v rámci realizace této smlouvy bude provedeno dle požadavků uvedených v návrzích novely ZKB a navazujících vyhlášek, které byly předloženy Poslanecké sněmovně ČR (dále PS ČR) ke schválení.

b) Pokud bude novela ZKB a navazující vyhlášky schválená PS ČR k dispozici v době realizace této zakázky, bude zavedený systém SŘBI plně v souladu se schváleným zněním této legislativy.

c) Zadavatel si uvědomuje, že pokud schválená novela ZKB a navazujících vyhlášek nebudou k dispozici v době realizace této zakázky a následně dojde ke změnám návrhů nové legislativy v průběhu schvalovacího řízení, bude nucen následně upravit zavedený SŘBI dle těchto změn. Tyto následné úpravy nejsou předmětem této zakázky.

d) Liberecká IS, a.s. se na zavedení nové legislativy v oblasti SŘBI již připravuje a v rámci této přípravy již:

1. Definovala aktiva společnosti
2. Definovala hrozby působící na aktiva společnosti
3. Provedla hodnocení rizik vyplývajících z definovaných hrozeb
4. Provedla návrh opatření k eliminaci definovaných rizik a stanovila „Strategii rozvoje služeb technické bezpečnosti pro informační systém statutárního města Liberec“

Název položky	Počty	Základní popis položky
Primární aktiva	14	Aplikační, systémové, telekomunikační služby, datové přenosy, bezpečnost IT, nákupy, lidské zdroje, materiální a finanční zdroje, řízení firmy, administrativa
Podpůrná aktiva	65	Rozpad z primárních aktiv, aplikace, dodavatelé, infrastruktura, úložiště atd.

Počet působících hrozeb celkem	44	Všechny typy působících hrozeb, jež jsou přiřazeny v rámci hodnocení rizik
Počet definovaných opatření k realizaci	27	Procesy, nákupy, zabezpečení atd.

Tyto podstatné aktivity pro zavedení SŘBI jsou v prostředí objednatele realizovány a proto následující aktivity zavedení SŘBI musí navázat na výše uvedené aktivity.

Objednatel nepožaduje zavedení systému bezpečnosti informací dle normy ISO 27001, protože tuto normu již ve svém prostředí implementovanou má!

Samotné zavedení systému řízení bezpečnosti informací pro pokrytí požadavků kybernetické bezpečnosti bude realizováno v rámci tří na sebe navazujících etap:

Etapa 0. – Zpracování a odsouhlasení cílového konceptu
Etapa I. – Implementace vybraných bezpečnostních opatření
Etapa II. – Interní audit kybernetické bezpečnosti

Zavedení systému řízení bezpečnosti informací a báze znalostí v oblasti KB v Liberecké IS a.s. bude zajištěno realizací následujících produktů:

Etapa 0.

Zhotovitel pro Objednatele vypracuje do 21 dnů od účinnosti této smlouvy cílový koncept a předloží jej Objednateli k odsouhlasení. Cílový koncept bude minimálně obsahovat:

a) Návrhy na úpravu časového harmonogramu jednotlivých etap plnění předmětu smlouvy dle přílohy č. 2 smlouvy (dále harmonogram).
b) Popisnou část, kde budou jednotlivé kroky a činnosti, případně vazby dle harmonogramu popsány;
c) Věcnou specifikaci jednotlivých etap plnění předmětu smlouvy dle harmonogramu, konkrétní plán prací a činností v jednotlivých etapách, které je nutné provést k úspěšné realizaci předmětu plnění této smlouvy. Obsahem bude také definice rolí jednotlivých zástupců Zhotovitele i Objednatele, podrobný postup dosažení jednotlivých etap, specifikace potřebných vstupů, milníky jednotlivých etap, testovací scénáře apod.;
d) Cílový koncept musí respektovat a zahrnovat všechny procesy, funkcionality, specifikace a požadavky stanovené v příloze č. 1 této smlouvy;
e) Obsah cílového konceptu musí být vzájemně prokazatelně odsouhlasen oběma smluvními stranami. Akceptace cílového konceptu Objednatelem je nezbytnou podmínkou pro zahájení dalších realizačních prací na plnění předmětu smlouvy.

Etapa I.

1. Řízení rizik

Je požadováno vytvoření a zavedení metodiky a procesů pro řízení rizik, plánu zvládání rizik a prohlášení o aplikovatelnosti (PoA). Procesy budou formalizovány v podobě notace BPMN jako součást procesní mapy kybernetické bezpečnosti.
Tvorba procesů bude realizována formou workshopu za účasti klíčových zainteresovaných stran dle pravidel procesního modelování.
Zavedením procesů se rozumí vznik dokumentace, příslušných registrů, rolí a záznamů při součinnosti garanta aktiva, vlastníka procesů, pod dohledem bezpečnostních rolí.

Výstupy - dokumenty:

- Příslušná část směrnice organizační bezpečnosti.
- Metodika pro identifikaci a hodnocení aktiv a pro hodnocení rizik – část rizika.
- Zpráva o hodnocení aktiv a rizik – část rizika.
- Prohlášení o aplikovatelnosti.
- Plán zvládání rizik.

2. Organizační bezpečnost

Je požadováno, aby výstupem tohoto produktu byl

- dokument - návrh a zavedení pravidel pro činnost Výboru pro řízení kybernetické bezpečnosti (včetně popisu rolí Manažer KB, Architekt KB, Auditor KB, Garant aktiva v souladu s VKB).

- vytvořen Výbor pro řízení kybernetické bezpečnosti a obsazeny bezpečnostní role vč. zajištění práv a povinností souvisejících s ISMS a ZKB / VKB.
- formální definice a jmenování do rolí požadovaných příslušnou vyhláškou kybernetické bezpečnosti.

Výstupy - dokumenty:

- Upřesnění obsahu bezpečnostních rolí (včetně udržování kontaktů s NÚKIB) v příslušné části směrnice organizační bezpečnosti.
- Jmenovací dekrety (bezpečnostních rolí).
- Jednací řád Výboru pro řízení kybernetické bezpečnosti

3. Řízení dodavatelů

Je požadováno vytvoření a zavedení procesu SLA managementu dodavatelů. Proces bude formalizován v podobě notace BPMN jako součást procesní mapy KB. Tvorba procesu bude realizována formou workshopu za účasti klíčových zainteresovaných stran dle pravidel procesního modelování.
Zavedením procesu se rozumí jeho pravidelné přezkoumání a případná aktualizace vlastníkem procesu, vznik a aktualizace příslušných registrů, záznamů o přezkoumání smluv a SLA a reportingu. (Registr významných dodavatelů, Zpráva o přezkoumání SLA).

Výstupy - dokumenty:

- Vytvoření procesu pro řízení dodavatelů z hlediska bezpečnosti informací v příslušné části směrnice organizační bezpečnosti.
- Návrh vzoru smlouvy pro dodavatele IT systémů splňující požadavky legislativy pro kybernetickou bezpečnost, a to pro „Výhradní dodavatele“ a „Nevýhradní dodavatele“.
- Záznam o přezkoumání smluv a SLA a reportingu

4. Řízení aktiv

Je požadováno vytvoření a zavedení metodiky pro řízení aktiv.
Procesy v metodice řízení aktiv budou formalizovány v podobě notace BPMN jako součást procesní mapy kybernetické bezpečnosti. Tvorba výstupů (identifikovaných a evidovaných aktiv včetně jejich metadat) bude realizována formou workshopu za účasti klíčových zainteresovaných stran dle pravidel procesního modelování.
V rámci definované metodiky řízení aktiv musí být obsaženy procesy vedoucí k pravidelnému přezkoumání (dopadové analýzy – §4 odst. 2, a-j) a případným aktualizacím evidovaných aktiv s jejich garanty a vlastníky spojených procesů. V rámci životního cyklu aktiva musí být také stanoven proces likvidace aktiv (dat a informací, vč. nosičů).

Výstupy - dokumenty:

- Vytvoření procesu pro řízení aktiv v příslušné části směrnice organizační bezpečnosti.
- Metodika pro identifikaci a hodnocení aktiv a pro hodnocení rizik – část aktiva.
- Evidence aktiv.
- Vzor zprávy o hodnocení aktiv a rizik

5. Bezpečnost lidských zdrojů

Je požadováno vytvoření plánu rozvoje bezpečnostního povědomí u lidských zdrojů subjektu s cílem zajistit odpovídající vzdělávání v patřičné formě, obsahu a rozsahu.
Procesy budou formalizovány v podobě notace BPMN jako součást procesní mapy kybernetické bezpečnosti. Tvorba procesů se bude týkat zajišťování odborných či pravidelných školení ve spojení s pracovní náplní rolí zaměstnanců, osob zastávajících bezpečnostní role, dále administrátorů a uživatelů. Realizace konkrétních školení není předmětem zadání.
Zavedením procesu se rozumí vznik dokumentace, popis rolí, vznik znalostní báze, vedení záznamů a kvalitní reporting. Určeny také musí být pravidla a postupy pro řešení případů porušení bezpečnostních politik od výše zmíněných rolí.

Výstupy - dokumenty:

- Příslušná část směrnice organizační bezpečnosti.
- Plán rozvoje bezpečnostního povědomí na rok 2026.
- Školící materiály (prezentace) pokrývající bezpečné chování uživatelů

6. Řízení provozu a komunikací

Je požadováno založení evidence bezpečného provozu IS / KS a stanovení pravidel a postupů s právy a povinnostmi rolí (administrátoři, uživatelé, osoby zastávající bezpečnostní role).
Dále je řešen vznik postupů pro sledování KBU / KBI, postupů pro ochranu přístupů k záznamům o těchto událostech.
Budou definována pravidla pro řízení technických zranitelností, pro ochranu před škodlivým kódem, pro řízení a schvalování provozních změn, postupy pro sledování, plánování a řízení kapacit lidských a technických zdrojů.
Budou definována pravidla pro zpracování informací a dat v průběhu jejich celého životního cyklu, vč. pravidelného zálohování a kontroly použitelnosti provedených záloh.
Budou popsány a zavedeny postupy pro instalaci technických aktiv a zajištění bezpečnosti síťových služeb, postupy pro spouštění a ukončení chodu IS / KS, vč. pravidel pro restart či obnovení chodu IS / KS s přihlédnutím k ošetření chybových stavů nebo mimořádných jevů.
Bude prověřeno zajištění oddělení vývojového, testovacího a provozního prostředí.

Výstupy - dokumenty:

- Příslušná část Směrnice technické bezpečnosti.
- Postupy pro instalaci technických aktiv a zajištění bezpečnosti síťových služeb, postupy pro spouštění a ukončení chodu IS / KS, vč. pravidel pro restart či obnovení chodu IS / KS s přihlédnutím k ošetření chybových stavů nebo mimořádných jevů.
- Evidence nepodporovaných technických aktiv.
- Topologie infrastruktury, prvků, koncových zařízení a serverů.
- Kontakty na osoby pověřené technickou a systémovou podporou

7. Řízení přístupů osob

Tento produkt zavádí bezpečný přístupový mechanismus k IS a KS u subjektu, vč. opatření k zajištění ochrany údajů používaných k přihlášení před zneužitím neoprávněnou osobou.
Evidence přístupových oprávnění bude řízena na základě skupin a rolí, každé osobě bude přidělen jedinečný identifikátor. Identifikátory budou také dedikovány pro aplikační a technické prvky, které s přidělenou rolí mohou nabývat přístupových práv a oprávnění.
Zavedena a bezpečně řešena budou také oprávnění pro mobilní a jiná technická zařízení subjektu a takových zařízení třetích stran, která nemá subjekt ve správě (dodavatelé, partneři, …).
Procesy spojené s evidencí přístupových oprávnění se zejména soustředí na aspekty privilegovaných oprávnění, pravidelného přezkumu nastavení veškerých přístupových oprávnění/skupin/rolí, správných postupů pro přidělování a odebírání oprávnění (počátek či ukončení smluvního vztahu s osobou, změna její role v rámci subjektu).
Vznikne dokumentace přidělování a odebírání přístupových oprávnění.

Výstupy - dokumenty:

- Příslušná část Směrnice technické bezpečnosti.
- Evidence přístupových oprávnění

8. Akvizice, vývoj, údržba / Řízení změn

Je požadováno vytvoření a zavedení procesů řízení sběru bezpečnostních požadavků a jejich provázání vůči procesům analýzy, vývoje a nasazení IT služeb pokrývajících obchodní požadavky zadavatele.
Procesy budou formalizovány v podobě notace BPMN jako součást procesní mapy kybernetické bezpečnosti. Tvorba procesů bude realizována formou workshopu za účasti klíčových zainteresovaných stran dle pravidel procesního modelování.
Je požadováno vytvoření a zavedení dokumentace, příslušných registrů, rolí a záznamů, institucionalizace standardu OWASP pro bezpečný vývoj a dalších bezpečnostních požadavků, záznamů a reportingu. (OWASP top ten, SDP).
Dokumentace bude zahrnovat pravidla pro udržování a využití vývojového a testovacího prostředí, vč. nasazení testovacích a testovaných dat a provedení bezpečnostního testování (penetrační testy) významných změn před jejich nasazením do provozu.
Je požadováno, aby při testování a uvedení do provozu nástroje (IS / KS) pro správu a ověřování identity bylo řešeno pomocí více faktorové autentizace, a to s nejméně 2 různými typy faktorů, při uvedení do provozu jiných aplikačních komponent. Následně bude rozhodnuto podle výsledků SAST, DAST, IAST, RASP.

Dokumentace bude zahrnovat pravidla pro včasné posouzení výsledků z dopadových analýz, které odhalí efekty z možné realizace významných změn a tak promítnou možná ovlivnění rizik, bezpečnostních politik, přinesou podklady pro druh otestování a také možnosti a postupy pro navrácení do původního stavu.
Součástí požadavků na vývoj, akvizici a správu musí být zejména:

- ✓ specifikace rizikových aktivit v aplikaci,
- ✓ zajištění monitorování a auditu rizikových aktivit,
- ✓ ověřování vstupních a výstupních dat technickými i organizačními opatřeními,
- ✓ kontrola vnitřního zpracování s důrazem na zachování jeho integrity,
- ✓ ochrana důvěrnosti, dostupnosti, integrity, autenticity a nepopiratelnosti odpovědnosti,
- ✓ ochrana informací při zpracování a jejich přenosu.
- ✓ stanovení požadovanou úroveň kryptografické ochrany,
- ✓ specifikace ochranu kryptografických prostředků s důrazem na kryptografické klíče,
- ✓ specifikace správy kryptografických prostředků.

Výstupy - dokumenty:

- Příslušná část Směrnice technické bezpečnosti.

9. Zvládání KBU / KBI

Je požadováno vytvoření a zavedení třech klíčových procesů pro zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů:

- ✓ Management monitoringu a událostí
- ✓ Incident management
- ✓ Problem management

Tyto procesy budou formalizovány v podobě notace BPMN jako součást procesní mapy KB. Tvorba procesů bude realizována formou workshopu za účasti klíčových zainteresovaných stran dle pravidel procesního modelování.
Je požadováno vytvoření a zavedení dokumentace, rolí a záznamů. Zavedením procesu se rozumí jeho pravidelné přezkoumání a případná aktualizace vlastníkem procesu, záznamů a reportingu.
Výstupy - dokumenty:

- Příslušná část Směrnice organizační bezpečnosti.
- Evidence událostí a incidentů.

10. Řízení kontinuity činností

Je požadováno vytvoření a zavedení procesu Managementu kontinuity služeb.
Proces bude formalizován v podobě notace BPMN jako součást procesní mapy KB. Tvorba procesu bude realizována formou workshopu za účasti klíčových zainteresovaných stran dle pravidel procesního modelování.
Je požadováno vytvoření a zavedení dokumentace, rolí a záznamů. Zavedením procesu se rozumí jeho pravidelné přezkoumání a případná aktualizace vlastníkem procesu,

Výstupy - dokumenty:

- Vytvoření procesu pro řízení kontinuity činností v rámci Směrnice organizační bezpečnosti.
- Plán kontinuity činností.
- Modelová osnova plánu obnovy pro vybraný IT celek.
- Formulář pro testování kontinuity

11. Bezpečnostní politika

Je požadováno vytvoření a zavedení základní souhrnné směrnice deklarující Bezpečnostní politiku a dokumentaci.
Oblasti zaváděných a tvořených pravidel bezpečnostních politik v členění dle paragrafů ZKB (oblasti nebudou obsahovat provozní činnosti, pouze návrh a zavedení procesů, postupů a související dokumentace).
Jsou požadovány návrhy procesů a zavedení procesů, postupů a související dokumentace ve složení:

- ✓ Politika ISMS,
- ✓ Politika řízení rizik,
- ✓ Politika organizační bezpečnosti,

- ✓ Politika řízení dodavatelů – stanovení bezpečnostních požadavků pro dodavatele,
- ✓ Politika řízení aktiv,
- ✓ Politika bezpečnosti lidských zdrojů,
- ✓ Politika řízení provozu a komunikací,
- ✓ Politika řízení přístupu osob,
- ✓ Politika akvizice, vývoje a údržby,
- ✓ Politika zvládání KBU / KBI,
- ✓ Politika řízení kontinuity činností,
- ✓ Politika kontroly a auditu,
- ✓ Politika fyzické bezpečnosti,
- ✓ Politika nástroje pro ochranu integrity komunikačních sítí,
- ✓ Politika nástroje pro ověřování identity uživatelů,
- ✓ Politika nástroje pro řízení přístupových oprávnění,
- ✓ Politika nástroje pro ochranu před škodlivým kódem,
- ✓ Politika nástroje pro zaznamenávání činnosti IS / KS, jeho uživatelů a administrátorů,
- ✓ Politika nástroje pro detekci KBU,
- ✓ Politika nástroje pro sběr a vyhodnocení KBU,
- ✓ Politika aplikační bezpečnosti,
- ✓ Politika kryptografických prostředků,
- ✓ Politika nástroje pro zajišťování úrovně dostupnosti informací,
- ✓ Politika bezpečnosti průmyslových a řídicích systémů,
- ✓ Politika zpracování osobních údajů,
- ✓ Zpráva z auditu kybernetické bezpečnosti,
- ✓ Zpráva z přezkoumání SŘBI,
- ✓ Metodika pro identifikaci a hodnocení aktiv a pro hodnocení rizik,
- ✓ Zpráva o hodnocení aktiv a rizik,
- ✓ Prohlášení o aplikovatelnosti,
- ✓ Plán zvládání rizik,
- ✓ Plán rozvoje bezpečnostního povědomí,
- ✓ Evidence změn,
- ✓ Hlášené kontaktní údaje,
- ✓ Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků.

Výstupy - dokumenty:

- Vytvoření nové bezpečnostní směrnice i s přílohami dle výše uvedeného členění vycházející z již zpracované dokumentace ISMS podle normy ISO 27001:

Etapa II.

Interní audit kybernetické bezpečnosti

Pro provedení interního auditu kybernetické bezpečnosti je požadováno:

- projednání způsobu provádění interních auditů ISMS, upřesnění auditovaných oblastí a procesů ISMS, jmenovaní auditorů,
- zpracování, projednání a vydání Programu interního auditu ISMS a Plánu interního auditu ISMS.
- provedení interního auditu ISMS:
  - ✓ příprava auditu – příprava auditních podkladů, upřesnění rámce a průběhu auditu a příprava jeho účastníků,
  - ✓ provedení auditu – shromáždění relevantních informací z auditovaných oblastí, jejich posouzení, zpracování a schválení ve formě auditních záznamů a příprava závěrů auditu z auditovaných oblastí,
    - audit ISMS bude proveden dle relevantních paragrafů VKB,
    - důraz bude položen na posouzení stavu zavedení opatření ISMS podle zpracované bezpečnostní dokumentace,
  - ✓ vyhodnocení auditu – bude zjištěna úroveň shody aktuálního stavu auditovaných oblastí se zvolenými kritérii auditu – požadavky návrhu VKB

V závěru bude provedeno roční přezkoumání ISMS s cílem přezkoumat celý systém.

Výstupy - dokumenty:

- Program interních auditů ISMS – program bude rozpracován na období 3 let,
- Plán interního auditu ISMS – plán obsahující činnosti připadající na jednotlivý audit,
- Zpráva z interního auditu ISMS, která obsahuje:
  - ✓ shrnutí zjištění, zhodnocení stavu bezpečnosti informací s uvedením neshod vůči požadovanému stavu,
  - ✓ přezkoumání zajišťování minimální úrovně kybernetické bezpečnosti obsahující vyhodnocení stavu ISMS (v předepsaném formátu),
  - ✓ o vyhodnocení bezpečnostních opatření z předchozího přezkoumání zajišťování minimální úrovně kybernetické bezpečnosti,
  - ✓ identifikace změn a okolností, které mohou mít vliv na zajišťování minimální úrovně kybernetické bezpečnosti,
  - ✓ zpětná vazba o účinnosti řízení bezpečnosti informací,
  - ✓ posouzení stavu plánu zavádění bezpečnostních opatření,
  - ✓ posouzení dopadů KBU / KBI na poskytované služby a kybernetickou bezpečnost,
  - ✓ posouzení změn s negativním dopadem na zajišťování minimální úrovně kybernetické
  - ✓ bezpečnosti,
  - ✓ identifikace možností pro neustálé zlepšování,
  - ✓ doporučení potřebných rozhodnutí, stanovení bezpečnostních opatření a osob zajišťujících výkon jednotlivých činností.

Příloha č. 2 smlouvy Harmonogram

LIBERECKÁ IS
NÁRODNÍ PLÁN OBNOVY

Příloha č. 7 ZD Zavedení systému řízení bezpečnosti informací a báze znalostí v oblasti KB

Dílčí položky předmětu smlouvy	Dílčí termíny pro plnění předmětu smlouvy								
	XII.24	I.25	II.25	III.25	IV.25	V.25	VI.25	VII.25	VIII.25
Etapa I.									
0. Cílový koncept	X								
1. Řízení rizik		X							
2. Organizační bezpečnost		X							
3. Řízení dodavatelů			X						
4. Řízení aktiv				X					
5. Bezpečnost lidských zdrojů				X					
6. Řízení provozu a komunikací					X				
7. Řízení přístupů osob					X				
8. Akvizice, vývoj, údržba / Řízení změn						X			
9. Zvládání KBU / KBI						X			
10. Řízení kontinuity činností							X		
11. Bezpečnostní politika							X		
Etapa II.									
Interní audit kybernetické bezpečnosti								X	X

Poznámka:

Označení křížkem znamená, že k poslednímu dni daného měsíce budou předány všechny výstupy požadované k daným položkám dle přílohy č. 1 uzavřené smlouvy.
Neúplné předání požadovaných výstupů k daným položkám ke konci uvedeného měsíce bude považováno za nedodržení dílčího termínu harmonogramu dle čl. V., odst. 4. smlouvy o poskytnutí služby