Příloha č. 1: Specifikace předmětu plnění

„**Zavedení systému řízení bezpečnosti informací a báze znalostí v oblasti a zpracování technické dokumentace“**

**Seznam zkratek:**

Objednatel Statutární město Liberec vč. městské policie Liberec

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

SML Statutární město Liberec

ISML Informační systém města Liberec

**Zavedení systému řízení bezpečnosti informací (dále SŘBI) a báze znalostí v oblasti kybernetické bezpečnosti v souladu s novým zákonem o kybernetické bezpečnosti (sněmovní tisk 759; 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 vytvořena strategie směřování Objednatele, budou stanoveny cíle SŘBI a popsány potřeby pro řízení zdrojů. Realizace předmětu smlouvy musí naplnit následující podmínky:

1. zavedení SŘBI v rámci realizace této smlouvy bude provedeno dle požadavků uvedených v návrzích ZKB a navazujících vyhlášek, které byly předloženy Poslanecké sněmovně ČR (dále PS ČR) ke schválení.
2. Pokud bude 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.
3. Zadavatel si uvědomuje, že pokud schválený ZKB a navazující vyhlášky 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.

Poznámka: Objednavatel má zřízenu akciovou společnost Liberecká IS a.s., jejíž primární úlohou je poskytování ICT služeb v prostředí Statutárního města Liberec. Liberecká IS a.s. spravuje z velké části (přibližně 90%) ICT služeb Objednavatele. Předmět plnění této zakázky se vztahuje pouze na k potřebám SŘBI Objednatele.

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

Etapa 0. – Zpracování a odsouhlasení cílového konceptu

Etapa I. – Analýza a revize aktuálních aktiv Objednatele

Etapa II. – Implementace vybraných bezpečnostních opatření

Etapa III. – Interní audit kybernetické bezpečnosti

**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:

1. Návrh časového harmonogramu jednotlivých etap plnění předmětu smlouvy.
2. Popisnou část, kde budou jednotlivé kroky a činnosti, případně vazby dle harmonogramu popsány;
3. 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.;
4. Cílový koncept musí respektovat a zahrnovat všechny procesy, funkcionality, specifikace a požadavky stanovené v tomto dokumentu;
5. 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.**

Zhotovitel pro Objednatele provede analýzu aktuálně zpracovaných primárních a podpůrných aktiv Objednavatele.

1. Analýza aktuálně zpracované evidence aktiv;
2. Vyhodnocení stavu evidence aktiv a návrhy na případné změny.
3. Akceptace navržených změn a realizace změn v definici aktiv.

**Výstupy:**

* Evidence aktiv v souladu s platnou legislativou ČR (strukturovaná databáze .csv, nebo .xls).

**Etapa II.**

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.

1. **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

1. **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

1. **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.

1. **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.

1. **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.  
Budou zavedeny a popsány opatření SŘBI pro mobilní zařízení.

**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

1. **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

1. **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.

1. **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.

1. **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

1. **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 zpracovaných dokumentací.

**Etapa III.**

**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.