SMLOUVA O POSKYTNUTÍ SLUŽBY A O DÍLO

Č. DS202503611

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

uzavřená podle zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

I. Smluvní strany

Objednatel:	**STATUTÁRNÍ MĚSTO LIBEREC**
	Nám. Dr. E. Beneše 1/1, 460 59 Liberec 1
zastoupené:	Ing. Jaroslavem Zámečníkem CSc., primátorem města
ve věcech smluvních:	Ing. Martinem Čechem, tajemníkem
ve věcech plnění smlouvy:	Ing. Zbyněk Vavřina, vedoucí odboru vnitřních věcí
IČO:	00262978
DIČ:	CZ00262978
bankovní spojení:	4096302/0800

(dále jen „objednatel“)

a

Zhotovitel:	**ATS-TELCOM PRAHA a.s.**
zastoupen:	Ing. Michalem Vančuříkem, předsedou představenstva
ve věcech smluvních:	Jindřichem Uhlářem, obchodním ředitelem
se sídlem:	Nad elektrárnou 1526/45, 106 00 Praha 10
IČO:	61860409
DIČ:	CZ 61860409
bankovní spojení:	Komerční banka a.s., č. ú. [redacted]

zapsaný v obchodním rejstříku vedeném u Městského soudu v Praze, oddíl B, vložka 2936

(dále jen „zhotovitel“)

II. Předmět a místo plnění

1) Touto smlouvou se zhotovitel zavazuje k provedení předmětu plnění a objednatel se zavazuje k převzetí předmětu plnění a zaplacení ceny za jeho provedení, a to za podmínek smluvených níže.
2) Předmětem plnění této smlouvy je zavedení systému řízení bezpečnosti informací (dále jen „SŘBI“) a báze znalostí v oblasti kybernetické bezpečnosti v souladu s novým zákonem o kybernetické bezpečnosti (sněmovní tisk 759) a Směrnicí evropského parlamentu NIS 2, a to v souladu s touto smlouvou a zadávací dokumentací veřejné zakázky „Zavedení systému řízení bezpečnosti informací a báze znalostí v oblasti a zpracování technické dokumentace“ (dále jen „veřejná zakázka“). V rámci realizace plnění dle této smlouvy 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 objednatele, dále bude vytvořena strategie směřování objednatele, budou stanoveny cíle SŘBI objednatele a popsány potřeby pro řízení zdrojů (dále též „předmět plnění“).

3) Předmět plnění je podrobně vymezen v Příloze č. 1 Specifikace předmětu plnění
4) Předmět plnění je rozdělen do těchto částí (etap), rovněž podrobně vymezených v Příloze č. 1 Specifikace předmětu plnění:
   - Etapa 0.
   - Etapa I.
   - Etapa II.
   - Etapa III.
5) Místo plnění: Nám. Dr. E. Beneše 1/1, 460 59 Liberec

III. Termín plnění

1) **Zahájení plnění**: nabytím účinnosti této smlouvy
2) **Ukončení plnění**: do 5 měsíců od nabytí účinnosti této smlouvy
3) Ukončení jednotlivých etap plnění dle čl. II. odst. 4 smlouvy je věcí organizace práce zhotovitele, závazný je pouze termín ukončení plnění dle předchozího odstavce.
4) Zhotovitel se zavazuje zahájit realizaci předmětu plnění ihned po nabytí účinnosti této smlouvy.
5) Za okamžik splnění se považuje den protokolárního předání předmětu plnění bez vad a nedodělků objednateli.

IV. Cena za předmět plnění

1) Cena za předmět plnění byla sjednána dohodou smluvních stran na základě cenové nabídky zhotovitele podané v rámci veřejné zakázky.

   Účastníky dohodnutá celková cena za celý předmět plnění činí:

Celková cena bez DPH:	**375 000,- Kč**
DPH 21%	**78 750,- Kč**
Celková cena s DPH:	**453 750,- Kč**

2) Cena za jednotlivé etapy plnění dle čl. II. odst. 4 smlouvy činí:

Název etapy	Cena bez DPH	DPH 21 %	Cena s DPH
Etapa 0.	37 500,-Kč	7 875,-Kč	45 375,-Kč
Etapa I.	37 500,-Kč	7 875,-Kč	45 375,-Kč
Etapa II.	262 500,-Kč	55 125,-Kč	317 625,-Kč
Etapa III.	37 500,-Kč	7 875,-Kč	45 375,-Kč

3) Celková cena za předmět plnění i jednotlivé etapy uvedená výše bez DPH (dále jen „celková cena") je smluvními stranami sjednána jako cena za celý předmět plnění i jednotlivé etapy vymezené v čl. II. smlouvy a jako cena nejvýše přípustná, platná po celou dobu realizace předmětu plnění, a to i v případě prodloužení lhůty plnění z důvodu na straně objednatele.
4) Celková cena zahrnuje veškeré náklady zhotovitele nezbytné k řádnému, úplnému a kvalitnímu provedení předmětu plnění včetně všech rizik a vlivů během realizace předmětu plnění. Celková cena zahrnuje předpokládaný vývoj cen v odvětví včetně předpokládaného vývoje kurzů české měny k zahraničním měnám až do doby dokončení a předání předmětu plnění. Celková cena zahrnuje též náklady na pojištění odpovědnosti za škody, bankovní garance, daně, cla, poplatky.
5) Objednatel je oprávněn odečíst z celkové ceny předmětu plnění částku skutečně neprovedených prací zhotovitelem ve výši položek uvedených v cenové nabídce, která tvoří přílohu této smlouvy.

V. Platební podmínky

1) Dohodnutá cena za jednotlivé etapy předmětu plnění bude ze strany objednatele uhrazena po řádném provedení a protokolárním předání a převzetí každé jednotlivé etapy na základě zhotovitelem vystavené celkové faktury s 30 denní splatností od data jejího prokazatelného předání objednateli.
2) Podkladem pro vystavení faktury bude soupis provedených prací nebo dodávek, oboustranně odsouhlasený a podepsaný osobami oprávněnými. Kopie podepsaného a vzájemně odsouhlaseného soupisu skutečně provedených prací nebo dodávek pověřenými pracovníky smluvních stran bude tvořit přílohu a součást příslušného daňového dokladu.
3) Veškeré účetní doklady musejí obsahovat náležitosti daňového dokladu dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Na faktuře bude uvedeno číslo smlouvy objednatele, název veřejné zakázky. V případě, že účetní doklady nebudou mít odpovídající náležitosti nebo pokud jejich přílohou nebude účastníky podepsaný soupis provedených prací, je objednatel oprávněn zaslat je ve lhůtě splatnosti zpět zhotoviteli k doplnění, aniž se tak dostane do prodlení se splatností; lhůta splatnosti počíná běžet znovu od opětovného zaslání náležitě doplněných či opravených dokladů.
4) Částka za provedení předmětu plnění bude zhotovitelem fakturována dle §92a a násl. zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, v režimu přenesené daňové povinnosti.
5) Zhotovitel prohlašuje, že prověřil skutečnosti rozhodné pro určení výše ceny předmětu plnění.
6) Tato smlouva nepřipouští překročení sjednané celkové ceny ani jakékoliv požadavky zhotovitele na úhradu vícenákladů oproti sjednané celkové ceně.

VI. Smluvní pokuty

1) Zhotovitel uhradí objednateli smluvní pokutu ve výši **0,2% z celkové ceny bez DPH za každý započatý den prodlení s termínem dokončení a předání celého předmětu plnění, bez omezení její celkové výše**.
2) Zhotovitel uhradí objednateli smluvní pokutu ve výši **0,1% z celkové ceny bez DPH** za každou vadu a započatý den v případě **prodlení s dohodnutým termínem na odstranění vad nebo nedodělků vyplývajících** z předávacího protokolu.
3) V případě **nedodržení kvalitativních parametrů prací a použitých materiálů** má objednatel právo účtovat zhotoviteli smluvní pokutu ve výši **1.000** Kč za každý jednotlivý případ.
4) V případě jakéhokoli **dalšího porušení této smlouvy nad rámec případů v tomto článku uvedených, má objednatel právo účtovat smluvní pokutu ve výši 500 Kč za každý den prodlení a jednotlivý případ porušení, pokud zhotovitel porušení neodstraní do 3 dnů** poté, co byl na porušení písemně upozorněn.
5) V případě opoždění objednatele s úhradou daňového dokladu má zhotovitel právo požadovat smluvní pokutu max. **ve výši 0,2 %** z nezaplacené částky za každý den prodlení. Objednatel není v prodlení s plněním své povinnosti platit cenu předmětu plnění, pokud je zhotovitel v prodlení s plněním kterékoliv své povinnosti dle této smlouvy.
6) Zaplacením smluvní pokuty není zhotovitel zbaven povinnosti příp. závady odstranit a předmět plnění předat v odpovídající kvalitě.
7) Zaplacením smluvních pokut nezaniká právo objednatele na náhradu škody.
8) Účastníci jsou oprávněni požadovat náhradu škody způsobené porušením povinnosti, na kterou se vztahuje smluvní pokuta, a domáhat se náhrady škody nehledě na částku uhrazené smluvní pokuty. Právo kterékoliv smluvní strany na náhradu škody vzniklé v souvislosti s porušením této smlouvy může být uplatněno samostatně.
9) Objednatel si vyhrazuje právo na úhradu smluvní pokuty formou zápočtu ke kterékoliv splatné pohledávce zhotovitele vůči objednateli.
10) Označil-li objednatel v reklamaci, že se jedná o vadu, která brání řádnému užívání předmětu plnění, případně hrozí nebezpečí škody velkého rozsahu (havárie), sjednávají obě smluvní strany smluvní pokuty v dvojnásobné výši.

VII. Odpovědnost za škody a pojištění

1) Zhotovitel na sebe přejímá zodpovědnost za škody způsobené všemi osobami a subjekty (včetně poddodavatelů) podílejícími se na provádění předmětu plnění, a to po celou dobu realizace.
2) Za tímto účelem má zhotovitel uzavřenu pojistnou smlouvu platnou po celou dobu realizace předmětu plnění na pojištění škod způsobených při výkonu činnosti třetí osobě, na škody vzniklé z jakékoliv příčiny, s hodnotou pojistného plnění přinejmenším odpovídající ceně předmětu plnění. Pokud zhotovitel tuto svoji povinnost nesplní, je objednatel oprávněn od této smlouvy odstoupit nebo sjednat vlastní pojistnou smlouvu s tím, že veškeré náklady a platby s tím spojené budou odečteny z celkové ceny předmětu plnění.
3) Zhotovitel nese riziko změny okolností ve smyslu ustanovení § 1765 občanského zákoníku.

VIII. Záruky

1) Záruka na předmět plnění je poskytována v délce 12 měsíců.
2) Zhotovitel je povinen provést veškeré práce související s realizací předmětu plnění v souladu s příslušnými právními předpisy a normami a v souladu s kvalitativními i kvantitativními požadavky objednatele uvedenými v zadávací dokumentaci veřejné zakázky, se kterou se zhotovitel před podpisem této smlouvy důkladně seznámil.
3) Pro odstraňování vad zjištěných při předání a převzetí předmětu plnění je nástup k odstranění těchto vad nejpozději do 15 dnů ode dne předání a převzetí předmětu plnění a odstranění těchto vad nejpozději do 15 dnů ode dne nástupu k odstranění vad, pokud nebude s ohledem na charakter vady se zástupcem objednatele dohodnuta lhůta delší.
4) Pro odstraňování vad v záruce je nástup k odstranění záruční vady nejpozději do 7 dnů ode dne jejího prokazatelného oznámení (např. z předávacího protokolu, elektronickou poštou) a odstranění těchto vad nejpozději do 15 dnů od jejich oznámení, pokud nebude s ohledem na charakter vady se zástupcem objednatele dohodnuta lhůta delší.

IX. Předání a převzetí předmětu plnění

1) Předání a převzetí předmětu plnění (jeho etapy) provede zástupce objednatele a zhotovitele, nebo osoba k tomu oprávněná v místě plnění předmětu plnění, a to na základě oboustranně podepsaného předávacího protokolu.
2) Objednatel souhlasí s předáním a převzetím jednotlivých částí předmětu plnění, ihned po jejich ukončení.
3) Objednatel souhlasí s předáním a převzetím předmětu plnění i před uplynutím smluvního termínu.
4) Současně budou předány veškeré doklady, potřebné pro uvedení předmětu plnění do trvalého užívání, zejména revize, licence, certifikáty, atesty.

X. Poddodavatelé

1) Zhotovitel je oprávněn využít pro zhotovení dílčích částí předmětu plnění spolupráce poddodavatelů. V každém případě zhotovitel odpovídá objednateli za řádnost a včasnost provedení předmětu plnění nebo porušení či škody, jako by toto prováděl sám.
2) Zhotovitel odpovídá objednateli, že poddodavatelé budou disponovat potřebnými oprávněními, odbornou kvalifikací a dostatkem odborných zkušeností pro provedení poddodávky, budou provádět předmět poddodávky sami přímo pro objednatele a že poddodavatelé nebudou ani část činnosti zadávat dalším poddodavatelům.
3) Zhotovitel v příslušné smlouvě uzavírané s kterýmkoliv poddodavatelem o provedení poddodávky zaváže poddodavatele k povinnosti dodržovat pokyny a instrukce objednatele. V případě pochybností objednatele o odbornosti či kvalitě prováděných prací poddodavatele, je objednatel oprávněn vyzvat zhotovitele k zastavení takových činností a žádat změnu poddodavatele.

XI. Ostatní ujednání

1) Pokud není ve smlouvě uvedeno jinak, řídí se smluvní strany příslušnými ustanoveními občanského zákoníku.
2) Obě smluvní strany prohlašují, že tato smlouva odpovídá jejich pravé vůli a že souhlasí s celým jejím zněním a na důkaz toho smlouvu vlastnoručně podepisují.

3) Tato smlouva je vyhotovena v elektronické podobě a bude podepsána oběma smluvními stranami prostřednictvím kvalifikovaného elektronického podpisu v souladu s nařízení eIDAS (Nařízení Evropského parlamentu a Rady (EU) č. 910/2014).
4) Smlouva nabývá platnosti dnem podpisu obou smluvních stran.
5) Smlouvu lze měnit či doplňovat pouze formou písemných, vzestupně číslovaných dodatků.
6) Objednatel i zhotovitel mají právo na odstoupení od smlouvy v případech, které předvídají právní předpisy, jimiž se řídí uzavřená smlouva.
7) Objednatel je oprávněn vypovědět smlouvu z důvodu porušení smlouvy ze strany zhotovitele. Účinnost takovéto výpovědi nastává dnem jejího doručení zhotoviteli.
8) Objednatel je oprávněn vypovědět smlouvu bez udání důvodu. Účinnost takovéto výpovědi nastává pátým dnem po jejím doručení zhotoviteli.

XII. Doložky

1) Smluvní strany berou na vědomí, že tato smlouva včetně metadat bude uveřejněna 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).
2) Smluvní strany berou na vědomí, že jsou povinny označit údaje ve smlouvě, které jsou chráněny zvláštními zákony (obchodní, bankovní tajemství, osobní údaje, …) a nemohou být poskytnuty, a to šedou barvou zvýraznění textu. Neoznačení údajů je považováno za souhlas s jejich uveřejněním a za souhlas subjektu údajů.
3) Smlouva nabývá účinnosti nejdříve dnem uveřejnění v registru smluv podle § 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).
4) 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.

XIII. Přílohy smlouvy

Přílohy této smlouvy tvoří:

1. Specifikace předmětu plnění

Za zhotovitele:

Ing. Michal Vančuřík
předseda představenstva

Za objednatele:

Ing. Martin Čech
tajemník

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:

a) 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.
b) 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.
c) 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:

a) Návrh časového harmonogramu jednotlivých etap plnění předmětu smlouvy.
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 tomto dokumentu;
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.

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

a) Analýza aktuálně zpracované evidence aktiv;
b) Vyhodnocení stavu evidence aktiv a návrhy na případné změny.
c) 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.

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. 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

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 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.