Příloha č.1

### **Specifikace Expertních služeb Manažera kybernetické bezpečnosti statutárního města Brna**

Dodavatel bude poskytovat pro zadavatele následující Expertní služby zahrnující následující dílčí plnění:

• Zajištění úkonů vyplývajících z povinností role manažera kybernetické bezpečnosti (dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti“) a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

• Plnění role Manažera kybernetické bezpečnosti v souladu s požadavky právních předpisů a převzetí role v organizaci.

• Odpovědnost za řízení a prosazování systému řízení bezpečnosti informací.

• Informování vedení organizace (popř. osob pověřených statutárním městem Brnem k řízení KB) o aktuálním stavu systému řízení bezpečnosti informací.

• Vedení pracovníků v týmu informační a kybernetické bezpečnosti organizace, koordinace jeho činností.

• Tvorba, prosazování a zajišťování aktualizace Bezpečnostní politiky informací.

• Tvorba, prosazování a zajišťování aktualizace dokumentace Systému řízení bezpečnosti informací dle požadavků zákona o kybernetické bezpečnosti a jeho prováděcích vyhlášek.

• Spolupráce při optimalizaci organizačního uspořádání informační a kybernetické bezpečnosti a návrhu budoucího modelu řízení informační a kybernetické bezpečnosti.

• Spolupráce při vytváření standardů informační a kybernetické bezpečnosti, konceptů plánů obnovy a dalších pravidel, včetně standardizace procesů informační a kybernetické bezpečnosti.

• Spolupráce při harmonizaci a optimalizaci nastavení procesů a činností informační a kybernetické bezpečnosti.

• Spolupráce při identifikaci aktuálního rozsahu a úplnosti informací o aktivech, identifikaci zdrojů, a návrhu na způsoby doplnění chybějících informací (information asset management).

• Spolupráce při procesu řízení rizik, jejich rozsahu a dopadu.

• Spolupráce při vytvoření katalogu služeb pro oblast informační a kybernetické bezpečnosti, tvorbě norem a standardů (SLA a KPI) v souladu s platnými právními předpisy a technickými normami.

• Podpora implementace nových procesů a zajištění přechodu na nové modely fungování informační a kybernetické bezpečnosti.

• Koordinace opatření ke zvýšení bezpečnostního povědomí v organizaci a školení zaměstnanců organizace v oblasti kybernetické bezpečnosti.

• Dohled nad Provozovateli a Významnými dodavateli z pohledu plnění požadavků zákona o kybernetické bezpečnosti a prováděcích předpisů – pravidelné informování a aktuálním stavu.

• Ověřování a vyšetřování kybernetických bezpečnostních incidentů, včetně zvládání kybernetických bezpečnostních událostí, a informování Výboru pro řízení kybernetické bezpečnosti statutárního města Brna o bezpečnostních incidentech, zjištěných neshodách a nedostatečné efektivnosti bezpečnostních opatření.

• Příprava podkladů pro realizaci bezpečnostních opatření (organizační a technická).

• Vyhodnocování vhodnosti a účinnosti bezpečnostních opatření.

• Spolupráce při auditech kybernetické bezpečnosti a jejich analýze.

• Vystupování jménem organizace k regulačním orgánům v oboru informační a kybernetické bezpečnosti.

• Při výkonu svojí funkce se řídí pokyny vedoucího Odboru městské informatiky/útvaru řízení kybernetické bezpečnosti.

Manažer kybernetické bezpečnosti zodpovídá za plánování, organizování a řízení realizace opatření, projektů a programů k řízení bezpečnosti informací tak, aby bylo dosaženo cílů stanovených zákonem o kybernetické bezpečnosti a jeho prováděcími předpisy, a to ve stanoveném termínu a v rámci stanoveného rozpočtu. Role Manažera kybernetické bezpečnosti působí jako „kontaktní“ osoba pro veškeré aspekty a otázky kybernetické bezpečnosti a prosazuje a koordinuje úlohu systému řízení informační bezpečnosti v organizaci.

**Pravomoci a odpovědnosti role**

Manažer kybernetické bezpečnosti je osoba odpovědná za systém řízení bezpečnosti informací od prevence přes průběžné testování až po eliminaci následků a vyhodnocení „úspěšných“ kybernetických incidentů. Odpovídá za tvorbu a aktualizaci Strategie kybernetické bezpečnosti a Bezpečnostní politiky informací.

Manažer kybernetické bezpečnosti je výkonným protějškem NÚKIB pro případy řešení kritických kybernetických bezpečnostních událostí.

Manažer kybernetické bezpečnosti bude zapojen ve všech důležitých projektech s dopadem na zpracování, přenos a ukládání informací, zavádění nových systémů nebo změny existujících systémů a procedur s dopadem do informační bezpečnosti ve fázi jejich přípravy a aplikace. Cílem tohoto opatření je zajistit, že budou náležitě vzaty do úvahy veškeré aspekty kybernetické bezpečnosti ve fázích přípravy, realizace a implementace všech relevantních projektů.

**Klíčové činnosti:**

* Účast na jednáních Výboru pro řízení kybernetické bezpečností statutárního města Brna.
* Odpovědnost za řízení systému řízení bezpečnosti informací.
* Pravidelný reporting pro vrcholové vedení zadavatele.
* Pravidelná komunikace s vrcholovým vedením zadavatele.
* Předkládání Zpráv o hodnocení aktiv a rizik, Plánu zvládání rizik a Prohlášení o aplikovatelnosti výboru pro řízení kybernetické bezpečnosti.
* Poskytování pokynů pro zajištění bezpečnosti informací při vytváření, hodnocení, výběru, řízení a ukončení dodavatelských vztahů v oblasti ICT.
* Komunikace s GovCERT/CSIRT.
* Podílení se na procesu řízení rizik.
* Koordinace řízení incidentů.
* Vyhodnocování vhodnosti a účinnosti bezpečnostních opatření