Formulář žádosti

o stanovisko Hlavního architekta eGovernmentu k plánovanému projektu zahrnujícímu záměr realizovat výdaj související s informačními a komunikačními technologiemi

(dle usnesení vlády ČR č. 86/2020 a/nebo zákona 365/2000 Sb.)

typ A

Odbor Hlavního architekta eGovernmentu DIA

Praha, květen 2024
verze 7.21

UPOZORNĚNÍ: Přestože je formulář zveřejněn ve formátu umožňujícím změny, žadatel není oprávněn měnit strukturu vybraných otázek či předepsaných odpovědí. Pokud se tak stane, Odbor Hlavního architekta eGovernmentu vyhodnotí takovou změnu jako porušení pravidel při schvalování a formulář bude vrácen bez vydání stanoviska. Tam, kde je to třeba pro uvedení dalších položek do tabulky, je žadatel oprávněn přidávat řádky pro tyto položky.

Metodický pokyn k vyplňování na adrese: https://archi.gov.cz/uvod_schvalovani#jake

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

1. ZÁKLADNÍ INFORMACE O PROJEKTU

1.1. Úvodní informace o žadateli o stanovisko k plánovanému projektu

Tabulka 1: **Úvodní informace o žadateli o stanovisko**				
Organizace žadatele	Městská část Praha 10		Vinohradská 3218/169, 100 00 Praha 10	00063941
Ředitel pro informatiku nebo Statutární zástupce	Lukáš Karásek	Vedoucí odboru informatiky	lukas.karasek@praha10.cz	+420 267 093 642
Kontaktní osoba projektu	Lukáš Karásek	Vedoucí odboru informatiky	lukas.karasek@praha10.cz	+420 267 093 642
Architekt projektu	Filip Šmehyl	IT konzultant	filip.smehyl@praha10.cz	+420 267 093 618

Verze předkládaných / doplněných žádostí o stanovisko, data jejich předložení a jejich čísla jednací		
Číslo předkládané verze:	**Datum předložení:**	**Verze předložena pod Čj,:**
1.6		

Tabulka 2: **Žádost o stanovisko dle (důvod žádosti)**	
Usnesení vlády č. 86, ze dne 27. ledna 2020 (U86)	***Ne***
Zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů (ZoISVS)	***Ano***
Výzva ESF (např. IROP) či jiných kofinancovaných programů (např. NPO), vypište číslo výzvy	*10. výzva IROP*
Dobrovolná žádost o stanovisko	***Ne***

1.2. Shrnutí charakteristik projektu

Tabulka 3: **Shrnutí charakteristik projektu**	
Název projektu:	**Zvýšení kybernetické bezpečnosti Úřadu městské části Praha 10**
Specifický cíl / účel projektu:	Hlavním cílem projektu je zvýšení kybernetické bezpečnosti a řízení rizik u aktiv MČP10, tj. jeho služeb, informací a informačních systémů. Tohoto cíle bude dosaženo realizací dílčích cílů zaměřených na řešení legislativních a regulatorních požadavků: • naplněná opatření organizačního a technického rázu odpovídající zákonu 181/2014 Sb. v rozsahu specifikovaném detailněji vyhláškou 82/2018 Sb. • začlenit problematiku zpracování osobních údajů v celé její šíři, což je rozsahem zákona 110/2019 Sb. • být v souladu s požadavky MBS (NÚKIB) ver. 1.2 (02/2023)
Seznam žádostí, které již byly v souvislosti s celkovými cíli a specifickým cílem / účelem projektu předány OHA:	• MV-216640/OHA-2022 - Dodávka a implementace FW pro 22 městských částí – příjemce HW/SW, uživatel Mepnet/KIVS pro přístup do CMS • DIA-6047/OHA-2023 - Dodávka, implementace a podpora technologie DC Interconnect – uživatel Mepnet/KIVS pro přístup do CMS
Odkazy na agendy VS, kterých se projekt týká:	Existuje agenda **A1721 Kybernetická bezpečnost**, avšak ZKB/VKB, a tedy působnost této agendy se na obce s rozšířenou působností vztahuje v tuto chvíli jen za předpokladu, že jsou správci významného informačního systému případně systému kritické infrastruktury nebo základní služby.

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

Tabulka 3: **Shrnutí charakteristik projektu**				
Seznam služeb veřejné správy z katalogu služeb veřejné správy (je možné uvést i kategorie služeb, pokud je celá kategorie relevantní)**, kterých se projekt týká:**		Nerelevantní, budou vytvářeny autonomní služby pro použití v rámci OVS		
Odkazy na určené IS dle UV 86/2020 a zákona 365/2000 Sb., kterých se projekt týká:	*Přímo dotčené určené IS, které projekt realizuje nebo mění*	-		
	Nepřímo dotčené určené IS	1756 E-spis, 1958 Gordic GINIS, 1959 VITA, 1960 PROXIO, 7319 - VITA Přestupky		
Názvy a odkazy na projekty v katalogu Digitálního Česka nebo jejich ID a názvy *Nebo informace, proč není součástí katalogu Digitální Česko. Financování z tohoto programu nehraje roli, jedná se o jednotný katalog všech ICT záměrů veřejné správy.*		Nerelevantní.		
Termíny:				
Předpokládané zahájení veřejné zakázky či zahájení realizace projektu:		**Spuštění první služby do produkčního prostředí:**	**Ukončení provozní smlouvy plánované v tomto projektu:**	
1.4.2025		**31.10.2025**	**31.10.2027**	
Výhrady ke zveřejnění formuláře:				
Formulář obsahuje veřejné informace a předpokládá se jeho zveřejnění. Pokud se zveřejněním nesouhlasíte, uveďte důvod, případně úpravy, které budou nutné, aby bylo zveřejnění možné:		**Nesouhlasíme se zveřejněním, formulář obsahuje údaje, které by mohly být zneužity třetími stranami a zapříčinit tak vznik KBU / KBI.**		
Výjimky:				
Žádáte výjimku/y vyplývající z nedodržení architektonických principů eGovernmentu nebo jiných skutečností?	***Ne***	**Počet žádostí o výjimku/y v přílohách:**	**0**	
Určení rolí věcného správce, technického správce, provozovatele a dodavatele (pokud je předmětem více IS, klasifikujte hlavní a ostatní vysvětlete v tabulce 8)**:**				
Věcný správce *Subjekt, který je investorem předmětu projektu*		MČP10 – garant primárních aktiv		
Technický správce *Subjekt, který zajišťuje technickou realizaci požadavků věcného správce k předmětu projektu*		MČP10 – garant podpůrných aktiv		
Provozovatel *Subjekt, který zajišťuje provoz HW a SW předmětu projektu*		MČP10 – provozovatel podpůrných aktiv		
Dodavatel *Subjekt, který dodává předmět projektu, pokud je znám v době přípravy projektu*		Konkrétní dodavatel výstupů bude vybrán na základě výběrového řízení v souladu se zákonem č. 134/2016 Sb. o zadávání veřejných zakázek.		
Bylo provedeno hodnocení ekonomické výhodnosti způsobu provozu určených IS? *Povinnost dle §5 odst. 2 písm. j) zákona č. 365/2000 Sb.*				***Ano*** *Studie proveditelnost, kap. 8, 9, 11*
Realizační (implementační) **výdaje v rámci projektu** (součet hodnot ve sloupci ① tabulky 55) **v Kč bez DPH:**				**57 850 774,-**
Provozní výdaje plánované v rámci projektu (součet hodnot ve sloupci ② tabulky 55) **v Kč bez DPH:**				**35 340 000,-**

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

1.3. Popis, potřebnost a výstupy projektu

Tabulka 4: **Popis projektu**

Popis výchozí situace projektu (tzv. As-Is, současný stav)**:**

Kontext organizace a její procesy kybernetické bezpečnosti

Požadavky z oblasti zajišťování kybernetické bezpečnosti nejsou v současné době v MČP10 systémově řešeny. Chybí definice systému řízení bezpečnosti informací (ISMS) a popis odpovědností, bezpečnostních rolí a základní bezpečnostní dokumentace včetně bezpečnostní politiky. Aktiva (primární a podpůrná) nejsou komplexně identifikována a řízena. Absence implementace ISMS vede mimo jiné k potenciálnímu rizikovému chování zaměstnanců MČP10 i jako celku, a v tom důsledku ke zvýšené míře výskytu KBU / KBI. V rámci MČP10 je snaha věnovat zajištění kybernetické bezpečnosti maximální pozornost a je předpokladem, že v průběhu tohoto zpracovávaného projektu bude provedeno hodnocení aktiv a rizik a dojde tak k podstatnému zlepšení stavu.

Z externí analýzy nesouladů se ZKB/VKB vyplývá aktuální zjištěný AS- IS stav s níže zmíněnými neshodami u těchto opatření:

ID	Organizační opatření	Hodnocení (As-Is)	Neshody (A/N)	Legislativa
O-01	ISMS (Systém řízení bezpečnosti informací)	**2**	A (9)	181/2014 Sb. § 5 2 a), 82/2018 Sb. § 3
O-02	Řízení rizik	**1**	N	181/2014 Sb. § 5 2 b), 82/2018 Sb. § 5
O-03	Bezpečnostní politika a dokumentace	**1**	N	181/2014 Sb. § 5 2 c)
O-04	Organizační bezpečnost	**1**	N	181/2014 Sb. § 5 2 d), 82/2018 Sb. § 6, 7 (Bezpečnostní role)
O-05	Stanovení bezpečnostních požadavků pro dodavatele (Řízení dodavatelů)	**1**	N	181/2014 Sb. § 5 2 e), 82/2018 Sb. § 8 (Řízení dodavatelů)
O-06	Řízení aktiv	**1**	N	181/2014 Sb. § 5 2 f), 82/2018 Sb. § 4
O-07	Bezpečnost lidských zdrojů	**2**	A (4)	181/2014 Sb. § 5 2 g), 82/2018 Sb. § 9
O-08	Řízení provozu a komunikací	**1**	N	181/2014 Sb. § 5 2 h), 82/2018 Sb. § 10
O-09	Řízení přístupů (osob)	**2**	A (2)	181/2014 Sb. § 5 2 i), 82/2018 Sb. § 12
O-10	Vývoj, akvizice, údržba (Řízení změn)	**1**	N	181/2014 Sb. § 5 2 j), 82/2018 Sb. § 13, 11 (Řízení změn)
O-11	Zvládání KBU / KBI[1]	**1**	A (3)	181/2014 Sb. § 5 2 k), 82/2018 Sb. § 14
O-12	Řízení kontinuity činností	**1**	A (3)	181/2014 Sb. § 5 2 l), 82/2018 Sb. § 15
O-13	Audit kybernetické bezpečnosti	**1**	N	181/2014 Sb. § 5 2 m), 82/2018 Sb. § 16

ID	Technická opatření	Hodnocení (As-Is)	Neshody (A/N)	Legislativa
T-01	Fyzická bezpečnost	**2**	A (2)	181/2014 Sb. § 5 3 a), 82/2018 Sb. § 17
T-02	Nástroj pro ochranu integrity komunikačních sítí	**2**	A (1)	181/2014 Sb. § 5 3 b), 82/2018 Sb. § 18
T-03	Nástroj pro ověřování identity uživatelů	**2**	A (1)	181/2014 Sb. § 5 3 c), 82/2018 Sb. § 19
T-04	Nástroj pro řízení přístupových oprávnění	**2**	A (1)	181/2014 Sb. § 5 3 d), 82/2018 Sb. § 20
T-05	Nástroj pro ochranu před škodlivým kódem	**2**	A (1)	181/2014 Sb. § 5 3 e), 82/2018 Sb. § 21
T-06	Nástroj pro zaznamenávání činnosti inf.komun. systému, jeho uživatelů a administrátorů	**2**	A (1)	181/2014 Sb. § 5 3 f), 82/2018 Sb. § 22
T-07	Nástroj pro detekci KBU / KBI	**2**	A (1)	181/2014 Sb. § 5 3 g), 82/2018 Sb. § 23
T-08	Nástroj pro sběr a vyhodnocení KBU / KBI	**1**	A (2)	181/2014 Sb. § 5 3 h), 82/2018 Sb. § 24
T-09	Aplikační bezpečnost	**2**	A (2)	181/2014 Sb. § 5 3 i), 82/2018 Sb. § 25
T-10	Kryptografické prostředky	**2**	A (2)	181/2014 Sb. § 5 3 j), 82/2018 Sb. § 26
T-11	Nástroj pro zajišťování úrovně dostupnosti informací	**1**	N	181/2014 Sb. § 5 3 k), 82/2018 Sb. § 27, 110/2019 Sb.
T-12	Bezpečnost průmyslových a řídících systémů	**1**	N	181/2014 Sb. § 5 3 l), 82/2018 Sb. § 28
T-13	Digitální služby	**1**	N	82/2018 Sb. § 29

Způsob hodnocení stavu pro obojí opatření byl definován níže uvedenou metrikou v rozmezí bodového systému (v závorce je pak počet neshod):

- ***1** – bezpečnostní činnosti a procesy nejsou realizovány*
- ***2** – bezpečnostní činnosti a procesy jsou definovány a realizovány částečně*
- ***3** – bezpečnostní činnosti a procesy jsou realizovány bez vyhodnocování*
- ***4** – bezpečnostní činnosti a procesy jsou realizovány a vyhodnocovány*

[1] **KBU, KBI** – Kybernetická bezpečnostní událost, Kybernetický bezpečnostní incident

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

Tabulka 4: **Popis projektu**

Řízení kvality:

Pozitivem v MČP10 je zavedení systému řízení kvality dle ISO 9001, ze kterého lze částečně vycházet při zavádění klíčových legislativních požadavků a opatření kybernetické bezpečnosti pro OVS[2], tedy dle legislativy ZKB/VKB[3] a ZZOÚ[4]. Tyto zdroje obsahují důležitá kritéria potřebná ke splnění a dlouhodobé udržitelnosti kybernetické bezpečnosti jako dynamického a fungujícího celku. MČP10 disponuje směrnicí Řízení HW a SW (prosinec 2022), která je součástí dokumentace QMS. Účelem této směrnice je:

- stanovit zásady provozování informačního systému MČP10 a informačních a komunikačních technologií
- stanovit jednotný a jednoznačný systém vedení, řízení, zodpovědnosti a identifikace HW/SW aktiv a jejich kontroly v průběhu životního cyklu
- stanovit odpovědnost za obsah, kvalitu a zveřejnění dokumentů na internetových stránkách MČP10

Popis cílové situace po dosažení celkového cíle / cílů projektu (tzv. To-Be, budoucí stav)**:**

Celkový cíl projektu, realizovaný jeho výstupy, je dosáhnout kvalitativního zlepšení v oblasti dynamicky vedené ISMS s podporou vrcholového vedení a se souladem se ZKB/VKB, popř. přípravou na splnění legislativních požadavků, které přinese přípravu na aplikování směrnice NIS2 po její lokální implementaci do ZKB. Velmi důležitým faktorem je dlouhodobá udržitelnost řešení a správné nastavení pravomocí a zodpovědností týkajících se kybernetické bezpečnosti.

Postupnými etapami tedy bude připravena ISMS politika zajišťování kybernetické bezpečnosti, dále stanovení strategie a cílů MČP10 v kybernetické bezpečnosti – samozřejmě v souladu s nadřízeným orgánem MHMP.

Implementací výstupů (*Tabulka 5 tohoto dokumentu*) dojde k podstatnému zvýšení kybernetické bezpečnosti aktiv MČP10, a to zejména informačních systémů a informací v nich obsažených za pomoci vhodných funkcí, procesů, služeb a nástrojů tvořených SW, HW a kvalitní bezpečnostní dokumentací.

Výstupem projektu tak není pouze prostá dodávka zařízení pro detekci incidentů, ale i rovněž zajištění schopností předcházet KBU a KBI v podobě preventivních opatření.

Zásadní změnou bude vybudování nového datového centra v geograficky oddělené lokalitě.

Důležitým výstupem projektu bude nejen vypracování bezpečnostní dokumentace, ale také ustavení procesů jejího udržování v aktuálním stavu a dalšího rozvoje. Tyto aktivity budou zajištěny externím subjektem, neboť žadatel nedisponuje dostatečnou kompetencí v oblasti problematiky kybernetické bezpečnosti a řízení rizik.

Bezpečnostní dokumentace bude obsahovat zpracované postupy a pravidla dle patřičných legislativních požadavků. Dalším krokem je zajištění a aplikování dostatečných znalostí o kybernetické bezpečnosti u dotčených zaměstnanců MČP10 prostřednictvím zajišťování pravidelných školení k problematice kybernetické bezpečnosti.

Dále bude pořízen potřebný SW / HW pro komplexní pokrytí oblastí kybernetické bezpečnosti při strategickém řízení rizik a udržitelnosti bezvýpadkových služeb, dostupných a ochraňovaných informací a aktiv MČP10.

Popis změn, tzn. výsledků / výstupů projektu nezbytných k dosažení jeho specifického cíle / účelu:

Důvody pro realizaci projektu

- **Zlepšit informovanost zaměstnanců o kybernetické bezpečnosti**: Zaměstnanci jsou často nejslabším článkem v kybernetické obraně. Proto je nezbytné, aby byli řádně proškoleni o kybernetických hrozbách a o tom, jak se jim bránit.
- **Získat možnost rychlejší reakce na kybernetické incidenty:** V případě kybernetického útoku je rychlá reakce klíčová pro minimalizaci škod. Dotace nám pomůže investovat do nástrojů a procesů, které nám umožní rychle identifikovat a reagovat na kybernetické incidenty.
- **Zlepšit správu celého cyklu softwaru:** Správa celého cyklu softwaru zahrnuje všechny fáze vývoje softwaru, od jeho návrhu až po jeho vyřazení z provozu. Dotace nám pomůže investovat do nástrojů a procesů, které nám pomohou zajistit, že náš software je bezpečný a odolný vůči kybernetickým útokům.

Očekávané výsledky / přínosy

- Snížení rizika kybernetických útoků
- Zlepšit naši schopnost reagovat na kybernetické incidenty
- Ochránit naše data a interní systémy
- Zvýšit důvěru našich klientů (občanů) a přispět k bezpečnosti metropolitní sítě

Závěr

Kybernetická bezpečnost je pro MČP10 klíčovou prioritou. Věříme, že projekt nám pomůže investovat do nástrojů a procesů, které nám pomohou chránit naše data a systémy před kybernetickými hrozbami.

[2] **OVS** – orgán veřejné správy
[3] **ZKB/VKB** – Zákon o kybernetické bezpečnosti 181/2014 Sb. a Vyhláška o kybernetické bezpečnosti 82/2018 Sb. v aktuálních zněních
[4] **ZZOÚ** - Zákon o zpracování osobních údajů 110/2019 Sb. v aktuálních zněních

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

Tabulka 4: **Popis projektu**
Přehled zvažovaných alternativ řešení rozdílných od „Popisu projektu“ (tzv. To-Be) **specifikovaného výše:**

Varianta 0

- Za nulovou variantu lze považovat zachování současného stavu, kdy projekt rozpracovaný ve Studii proveditelnosti nebude realizován. Z ekonomického hlediska nulová varianta zdánlivě šetří přímé investice, nepřináší ale žádné kvalitativní benefity, úroveň rizika neklesá. Vlastní potvrzení realizace projektu, nebo zachování nulové varianty, je otázkou pro vedení MČP10, ideálně se zohledněním výstupů a závěrů zpracované Studie proveditelnosti.
- Při nulové variantě nebude žadatel kybernetickou bezpečnost dále rozvíjet. Nulová varianta povede k tomu, že žadatel nebude dostatečně připraven na kybernetické hrozby. Pokud se žadatel nebude rozvíjet v oblasti kybernetické bezpečnosti, tak sice ušetří finanční prostředky, ale zvýší se pravděpodobnost útoků a hrozeb, na jejichž odstranění mohou být vynaloženy finanční prostředky výrazně vyšší.
- Rizika vyplývající z nulové varianty jsou tak zásadní (s potenciálně dramatickým dopadem na rozpočet městské části), že vedení MČ rozhodlo projekt za pomoci IROP 21+ připravit.

Varianta 1– Provozní varianta

- Při zachování status quo nebude žadatel dostatečně připraven na rizika v oblasti kybernetické bezpečnosti. Bez neexistujících bezpečnostních politik nelze zajistit dodržování opatření, kterými by se předcházelo kybernetickým bezpečnostním incidentům. Bez nastavení a definování procesů bezpečnostní politiky nelze zajistit ochranu příslušných aktiv. V případě bezpečnostního incidentu tak bude žadatel vystaven velkému nebezpečí odcizení dat, případně poškození důležitých aplikací informačního systému.

Varianta 2 – Postupný rozvoj

- Postupný upgrade současných SW, HW komponent, postupná implementace organizačních opatření. Realizace by proběhla „neprojektovou“ formou, tj. postupně, po částech, dle finančních, personálních a časových možností. Výhodou takového řešení je rozložení investice v čase (nižší tlak na rozpočet městské části). Nevýhod takového řešení je celá řada, mezi nejvýznamnější určitě patří praktická nemožnost dotačního financování (tím pádem vyšší tlak na vlastní rozpočet pohledem celkové investice), nemožnost zásadně povýšit kybernetickou bezpečnost žadatele v časově rozumném horizontu, nejistota zajištění financování v čase (politický cyklus).

Varianta 3 – Nezávislost na stávajícím stavu

- Toto alternativní řešení projektu spočívá ve vybudování dvou redundantních technologických center (TC) tzv. „na zelené louce“ a následný přechod ze stávajícího TC. Toto řešení však není ve střednědobém časovém horizontu a s ohledem na předpokládané náklady (násobně vyšší, než je předkládané projektové řešení) realizovatelné.

Varianta 4 – Rozvojová projektová varianta

- Rozvojová varianta je postavena na jednorázovém povýšení současného stavu kyberbezpečnosti žadatele na vyšší úroveň dle stanovených cílů, tj. realizací předkládaného projektu. Realizace proběhne formou projektu, tj. ve stanoveném čase, s předem definovanými náklady, projektovým týmem a definovanými výstupy.
- Realizací projektu dojde k odstranění nejpalčivějších problémů kybernetické bezpečnosti žadatele. Cílový stav počítá s kvalitně zpracovanými bezpečnostními politikami, nastavenými procesy a pravidly, která budou uplatňována v praxi a přispějí k větší bezpečnosti informačního systému a jednotlivých aplikací a snížení rizika výskytu bezpečnostních incidentů.
- Díky realizaci pomocí projektu bude značně sníženo riziko poškození informačních systémů, případně odcizení dat.

Tabulka 5: **Přehled výstupů projektu**

Označení výstupu	**Množství a jednotka**	**Celková cena výstupu** [Kč]	**Plánovaná životnost výstupu [rok]**	**Vysvětlení výstupu**
V-01 FC Switch	4 ks	2.662.000,-	5	Fibre Channel (FC) switch. Fibre Channel technologie pro přenos dat v úložných systémech a serverových sítích. Celkové hardwarové řešení musí zajistit dostatečnou odolnost pro hardware failure jednotlivých nodů a dostatečný výkon pro provoz požadovaných aplikací. **Opatření (legislativní požadavky): T-02**
V-02 LAN ToR Switch	8 ks	3.388.000,-	5	Top of Rack (ToR) switch - síťové zařízení, které bude umístěné na horní části (top) datového stojanu nebo regálu v datovém centru. Cílem je minimalizovat délku síťových kabelů mezi servery a síťovým přepínačem, což může vést ke snížení latence a zjednodušení infrastruktury. **Opatření (legislativní požadavky): T-02**
V-03 LAN management Switch	2 ks	363.000,-	5	Síťové zařízení s metalickými porty, do kterého se připojí management konzole jednotlivých datacenter prvků. Využití ke vzdálené administraci serverů a dalších serverových částí. **Opatření (legislativní požadavky): T-02**
V-04 NG Firewall	3 ks	2.360.000,-	5	NGFW s pokročilými bezpečnostními funkcemi pro ochranu perimetru a interní sítě. Zajišťuje filtrování provozu na základě parametrů určených pro jednotlivé síťové vrstvy. Propojuje jednotlivé segmenty sítě a zajišťuje pokročilou filtraci a ochranu

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

Tabulka 5: **Přehled výstupů projektu**				
Označení výstupu	**Množství a jednotka**	**Celková cena výstupu** [Kč]	**Plánovaná životnost výstupu [rok]**	**Vysvětlení výstupu**
				provozu. Funguje jako jednotný vstupní bod do napojených infrastruktur. NGFW throughput alespoň 10 Gbps. **Opatření (legislativní požadavky): T-02**
V- 05 Webový aplikační FW	1 ks	787.000,-	5	WAF, který chrání webové aplikace a API před širokou škálou hrozeb: • Filtrování webového provozu • Detekce a prevence zranitelností • Pravidla pro blokování a povolení • Učení se a adaptace **Opatření (legislativní požadavky): T-02, T-09**
V-06 Nástroj pro VPN	1 ks	787.000,-	5	Nástroj pro zajištění virtuální privátní sítě (VPN), která poskytuje zabezpečené a šifrované připojení mezi klientským koncovým zařízením a sítí organizace prostřednictvím sítě internet. **Opatření (legislativní požadavky): T-03, T-04**
V-07 Nástroj pro vícefaktorvé ověřování	1 ks	2.118.000,-	5	Systém vícefaktorového ověřování musí podporovat kombinaci několika metod ověření identity uživatele pro zvýšení bezpečnosti přístupu k aplikacím a uživatelským účtům na koncových zařízeních. Systém by měl být kompatibilní s běžně používanými operačními systémy (Windows, Linux, MacOS). Systém musí být uživatelsky přívětivý, minimalizovat dopad na běžné pracovní procesy a zároveň zachovat vysokou úroveň zabezpečení. Systém by měl umožňovat nastavení různých časových intervalů pro vynucení opětovného ověření a měl by umožňovat nastavit nevynucované ověření v případě připojení uživatele z lokální sítě úřadu. Kromě zadání tradičního hesla nebo PIN kódu musí systém umožnit vyžádání druhého faktoru ověření. **Opatření (legislativní požadavky): T-03**
V-08 Nástroj pro detekci KBU	1 ks	6.958.000,-	5	Nástroj pro monitoring provozu v rámci datové sítě a koncových zařízení s identifikací nestandardního či nežádoucího chování. Automatizovaná detekce a reakce na události na síti i koncových bodech. Poskytovaní maximální visibility, podpory vyhodnocování a validace alarmů s vylepšenou reakcí v reálném čase i do minulosti. Zvýšení efektivity a účinnost zabezpečení sítě. Rozšířené možnosti detekce a reakce na hrozby (XDR). • Zabezpečení sítě (NDR) - monitoring, detekce, reakce, proaktivní ochrana, hloubková inspekce, sendboxing, rozpoznání infiltrace, monitoring laterálního pohybu, detekce malware v šifrovaném provozu. • Zabezpečení koncových bodů (EDR) - monitoring a analýza činnosti, reakce na incidenty a rychlé odstranění nebo omezení hrozeb, integrace na feedy hrozeb, forenzní vyšetřování. • Síťové pasti - nasazení autentických vrstev nástrah, které pomohou identifikovat útok a umožní získat přehled o nebezpečné aktivitě - mechanismy detekce a včasných výstrah, včetně analýzy v sandboxu. **Opatření (legislativní požadavky): T-07**
V-09 E-mail protection	1 ks	1.785.000,-	5	Systém pro ochranu e-mailové komunikace zajišťující ochranu proti spamu (antispam), virům (antivirus) a malicious softwaru na základě signatur. Ochrana pro přibližně 600 emailových schránek. **Opatření (legislativní požadavky): T-02**
V-10 Nástroj na sběr a vyhodnocování logů	1 ks	2.148.000,-	5	LogManagement s neomezeným sběrem logů: • Zpracování událostí z různých zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware. • Možnost dopsání parseru pro zařízení aktuálně nepodporované výrobcem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému. • Systém standardizuje přijaté logy do jednotného formátu a logy jsou parserovány (rozdělovány) do příslušných políček dle jejich typu. • Nad takto standardizovanými daty systém automaticky vytváří indexy pro rychlejší vyhledávání pro všechna pole standardizovaného logu.

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

Tabulka 5: **Přehled výstupů projektu**				
Označení výstupu	**Množství a jednotka**	**Celková cena výstupu** [Kč]	**Plánovaná životnost výstupu [rok]**	**Vysvětlení výstupu**
				• Všechny rozparsované položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem. • Systém nesmí umožnit mazání nebo modifikování již uložených logů. • Konsolidace logů na centrálním místě. • Snadné vyhledávání událostí (ad hoc) bez nutnosti programování. • Grafické znázornění událostí (grafy událostí). • Grafické znázornění TOP událostí nad všemi daty za určité časové období. • Automatické doplňování GeoIP informací k událostem a jejich grafické znázornění na mapě. • Automatické doplňování reverzních DNS záznamů k IP adresám. • V případě přetížení systému jsou události ukládány do vyrovnávací paměti. • Unifikované vyhledávání napříč všemi typy dat a zařízení. **Opatření (legislativní požadavky): T-07, T-08**
V-11 SIEM	1 ks	6.958.000,-	5	Systém pro správu bezpečnostních informací a událostí. Analytický software, který sbírá a koreluje události z bezpečnostních a síťových zařízení, případně z aplikací. Dokáže identifikovat podezřelé události, jako jsou stažení souborů nebo příliš vysoký přenos informací. Trvalé zpracování 2500 událostí za sekundu a online dostupná data po dobu 6 měsíců, automatický alerting, možnost generování reportů, možnost forenzního vyšetřování. Schopnost integrace na další bezpečnostní prvky. **Opatření (legislativní požadavky): T-07, T-08**
V-12 Technologický aplikační monitoring	1 ks	2.118.000,-	5	Jednotná platforma pro visibilitu incidentů ze všech security řešení. Systém pro pokročilé IT monitorování a řízení infrastruktury bude navržen tak, aby poskytoval detailní a současně strukturovaný pohled na provoz IT infrastruktury a aplikací v organizaci. Tento systém bude schopen kontinuálně shromažďovat a analyzovat data z různých existujících dohledových systémů (Zabbix), což umožní rychlé a efektivní vyhodnocení aktuálního stavu infrastruktury a aplikací. Bude možné definovat závislosti jednotlivých prvků IT provozu, což usnadní identifikaci provozních celků a jejich schopnosti poskytovat služby. V případě potřeby budou pracovníci dohledu moci snadno zjistit, kde v řetězci zdrojů, závislostí a samotného systému došlo k problémům, což umožní rychlou a cílenou reakci. Systém bude uchovávat shromážděné informace a generovat pravidelné management reporty, které poskytnou důležité informace pro řízení IT infrastruktury. Tyto reporty budou zahrnovat data za vybrané časové období a umožní tak sledování vývoje a optimalizaci IT prostředků. **Opatření (legislativní požadavky): T-07, T-08**
V-13 DLP	1 ks	2.239.000,-	5	Nástroj pro monitoring práce s daty a soubory a ochranou před ztrátou. Systémový přístup k monitorování a ochraně citlivých dat díky nástroji DLP zabezpečuje proti únikům, krádeži a neoprávněnému sdílení. **Opatření (legislativní požadavky): T-07, T-08**
V-14 Nástroj pro vulnerability skenování	1 ks	1.301.000,-	5	Nástroj pro snadné vytváření skenovacích úloh, samostatné vyhledání otevřených vstupních bodů do skenovaných entit - otevřené porty, publikované služby, automatické doplnění rozšiřujících informací o nalezených zranitelnostech v čem zranitelnost spočívá, jaká je její obecná závažnost, odkazy na další uveřejněné informace výrobců. Schopnost plánovaného spouštění úloh. Notifikace do mailu po skončení skenovací úlohy. Řízení rychlosti probíhání skenů, limitace souběžných spojení. Reportovací funkce dle různých hledisek, podle zranitelností, podle hostů apod. **Opatření (legislativní požadavky): T-09**

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

Tabulka 5: **Přehled výstupů projektu**				
Označení výstupu	**Množství a jednotka**	**Celková cena výstupu** [Kč]	**Plánovaná životnost výstupu [rok]**	**Vysvětlení výstupu**
V-15 Nástroj pro správu privilegovaných účtů	1 ks	2.538.000,-	5	Nástroj na řízení a správu privilegovaných účtů administrátorů jak interního IT, tak dodavatelů (PIM/PAM). Nástroj umožňující získat kontrolu nad rutinními operacemi s privilegovaným přístupem. **Opatření (legislativní požadavky): T-03, T-04**
V-16 Nástroj na sběr a vyhodnocování logů z firewallů	1 ks	1.198.000,-	5	Nástroj pro centrální logování provozních a systémových dat z centrálního a pobočkových firewallů. Umožňuje přehlednou vizualizaci provozních dat na základě vydefinovaných filtrů, tvorbu statických i dynamických reportů, dohledávání událostí na základě definovaných parametrů. **Opatření (legislativní požadavky): T-06, T-08**
V-17 Sandbox	1 ks	2.166.000,-	5	Systém pro detekci 0-day zranitelností v analyzovaných souborech, které do systému automatizovaně zasílají ostatní systémy v rámci řešení. Systém simuluje spuštění/otevření souboru v koncové stanici a sleduje dopady chování souboru na systém jako celek. **Opatření (legislativní požadavky): T-07**
V-18 Server	10 ks	3.751.000,-	5	Servery pro virtualizaci, hardware pro zajištění provozu všech virtualizovaných serverů. Celkové hardwarové řešení musí zajistit dostatečnou odolnost proti hardware failure jednotlivých nodů a dostatečný výkon pro provoz požadovaných aplikací ve dvou lokalitách kvůli geografické redundanci. **Opatření (legislativní požadavky): T-11**
V-19 Server pro SDS	10 ks	3.509.000,-	5	Servery pro softwarově definovanou storage (SDS) CEPH (objektové, blokové a souborové úložiště) hardware pro zajištění provozu horizontálně škálovatelného clusteru - uložiště dat všech virtuálních serverů vyjma databázových. Celkové hardwarové řešení musí zajistit dostatečnou odolnost proti hardware failure jednotlivých nodů a dostatečný výkon pro provoz požadovaných aplikací ve dvou lokalitách kvůli geografické redundanci. **Opatření (legislativní požadavky): T-11**
V-20 Storage SAN	2 ks	8.107.000,-	5	Full flash diskové úložiště pro produkční a testovací databázové systémy. Storage jsou specializované úložištní systémy pro efektivní a výkonné správy a ukládání dat. Mimo jiné fungují jako úložiště pro jednotlivé virtuální servery. Celkové hardwarové řešení musí zajistit dostatečnou odolnost proti hardware failure a dostatečnou kapacitu pro provoz požadovaných aplikací ve dvou lokalitách kvůli geografické redundanci (1 primární lokalita, 1 sekundární lokalita). Připojení přes Fibre channel porty. **Opatření (legislativní požadavky): T-11**
V-21 Zálohování	1 ks	2.118.000,-	5	Zálohovací nástroj bude použit pro pravidelné zálohování dat a systémových konfigurací. Zároveň je požadováno zajištění záloh prostředí MS Office 365 (E3). Cílem je zajistit rychlou a efektivní obnovu v případě výpadku, havárie nebo jiných neočekávaných situací, které mohou ohrozit data nebo dostupnost služeb. **Opatření (legislativní požadavky): T-11**
V-22 Endpoint security management	1 ks	2.057.000,-	5	Software pro jednotnou a komplexní správu a zabezpečení koncových bodů, který IT administrátorům umožňuje spravovat, chránit a zabezpečit stolní počítače, notebooky, servery a další koncové body v síti. **Opatření (legislativní požadavky): T-02, T-05**
V-23 Ochrana a správa mobilních zařízení - MDM	1 ks	1.072.000,-	5	Software pro kompletní správu a zabezpečení mobilních zařízení (MDM). Rozsah podporovaných zařízení zahrnuje mimo jiné smartphony, tablety a notebooky. Systémy podporované aplikací jsou alespoň Apple (iOS, iPadOS), Android, Windows, Chrome OS. Konfigurace systému je intuitivní, každodenní správcovská obsluha je podporována interaktivními dashboardy viditelnými ihned po přihlášení do Mobile Device Manageru. Administrátor získá přístup k informaci o aktuálních problémech, kondici a způsobu využívání zařízení. **Opatření (legislativní požadavky): T-02, T-05, T-06, O-09**
V-24 EZS serverovna	1 ks	569.000,-	5	Samostatný elektronický zabezpečovací systém (EZS) pro zabezpečení serverovny napojený na elektronický přístupový systém: • Magnetický kontakt na vstupní dveře

Tabulka 5: **Přehled výstupů projektu**				
Označení výstupu	**Množství a jednotka**	**Celková cena výstupu** [Kč]	**Plánovaná životnost výstupu [rok]**	**Vysvětlení výstupu**
				• Pohybový senzor pro detekci pohybu v neautorizovaných časech • Externí alarm o narušení prostoru pro ostrahu • Oznamovací systém pro informování formou SMS o narušení zabezpečení pro alespoň 5 kontaktů • Systém musí komunikovat šifrovaně a bezpečně • Možnost napojení celého systému na lokální Ethernetovou síť (RJ45) pro případnou správu ze serveru **Opatření (legislativní požadavky): T-01**
V-25 Kamerový systém serverovna	1 ks	400.000,-	5	Samostatný kamerový systém pro serverové prostory: • 1x 365 kamera se sledováním pohybu nebo 2x standardní kamera • Rozlišení alespoň 1080p • Kamery s nočním viděním • Podpora Ethernetu s RJ45 konektorem a PoE • Možnost vzdáleného připojení pro zobrazení živého obrazu nebo archivovaných záznamů • Rozpoznávání obličejů a zaslání notifikace v případě neautorizované osoby v objektu • NVR pro uložení záznamů z kamer po dobu alespoň 60 dní • Šifrovaná a bezpečná komunikace mezi kamerami a NVR **Opatření (legislativní požadavky): T-01**
V-26 Elektronický přístupový systém serverovna	1 ks	426.000,-	5	Samostatný elektronický přístupový systém napojený na EZS: • Čtečka umožňující kombinaci karty (MIFARE S50) + PIN kódu • Řídící jednotka pro přístupový systém umožňující integraci s EZS • Kapacita řídící jednotky alespoň 50 karet pro autorizaci uživatelů • Možnost programování a správy přístupů přímo na řídící jednotce nebo prostřednictvím SW • Schopnost uchovávat logy o přístupech pro auditní účely • Systém musí komunikovat šifrovaně, bezpečně a zamezit přístupu do prostor bez autorizace • Možnost napojení celého systému na lokální Ethernetovou síť (RJ45) pro případnou správu ze serveru **Opatření (legislativní požadavky): T-01**
V-27 Serverová UPS	1 ks	1.174.000,-	5	Modulární UPS s výkonem alespoň 75 kW rozděleno do alespoň 3 jednotek o výkonu minimálně 25 kW: • Možnost přidávání nebo odebírání jednotek (modulů) za chodu • Vhodné pro dlouhodobé zálohování a kontinuální provoz • Vhodné pro použití v kombinaci s diesel agregátem • Pokročilé řízení baterií pro optimalizaci výkonu a prodloužení jejich životnosti • Možnost napojení UPS na lokální Ethernetovou síť (RJ45) pro monitoring stavu a vzdálený přístup k informacím • Ochrana proti přepětí a napěťovým špičkám • Přepnutí do bypass režimu při detekci přetížení **Opatření (legislativní požadavky): T-01**
V-28 Penetrační testy	1 ks	363.000,-	-	Provedení penetračních testů po implementaci nových HW/SW nástrojů. **Opatření (legislativní požadavky): O-13**

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

1.4. Právní klasifikace specifického cíle / účelu projektu

Tabulka 6: **Klasifikace specifického cíle / účelu projektu dle legislativy eGovernmentu (pokud je v rámci projektu realizováno více IS, klasifikujte hlavní a ostatní vysvětlete)**		
Klasifikace	**Vyberte**	
Druh informačního systému dle klasifikace zák. č. 365/2000 Sb., o informačních systémech VS	**Provozní informační systém nepodléhající zák. 365/2000 Sb.**	
Je projektem dotčen (tj. realizován nebo na úrovni jeho procesní a aplikační architektonické vrstvy měněn) určený informační systém dle zák. č. 365/2000 Sb., o informačních systémech VS?	**Ano - VYPLŇTE DLE JAKÉHO KRITÉRIA**	☐ 1. Využívá služby referenčního rozhraní nebo poskytuje služby referenčnímu rozhraní ☑ 2. Má vazbu na systém dle bodu 1 ☐ 3. Je určený k poskytování služby fyzickým nebo právnickým osobám s předpokládaným počtem uživatelů, kteří využívají přístup se zaručenou identitou, alespoň 5000 ročně
Je projektem dotčen agendový informační systém dle zákona č. 111/2009 Sb., o základních registrech?	**Ano**	
Budou informačním systémem, který je projektem dotčen, přijímány a odesílány datové zprávy dle zák. č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů?	**Ano**	
Druh informačního / komunikačního systému dle klasifikace stanovené zákonem č. 181/2014 Sb., o kybernetické bezpečnosti	**Nespadá pod definici dle ZoKB**	
Bezpečnostní úroveň informačního systému dle vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci	**Bezpečnostní úroveň neurčena**	

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

1.5. Přínosy (celkový cíl / cíle) projektu

Tabulka 7: **Strukturovaný přehled přínosů (celkového cíle / cílů) projektu včetně uvedení objektivně ověřitelných ukazatelů jejich dosažení a zdrojů a prostředků jejich ověření**

Přínosy na straně uživatelů (např. snížená časová nebo administrativní náročnost oproti vyřízení aktivity dosavadním způsobem, vyšší ochrana osobních dat aj.)**:**

Nejdůležitějším přínosem na straně uživatelů (zaměstnanců územního samosprávného celku), pracujících s IS, tedy službami spravovanými MČP10, bude zvýšení jejich informovanosti o možných kybernetických rizicích. To jim v případě potřeby umožní proaktivně reagovat, včas se společně vypořádat se s KBU / KBI, ale spíše jim dostatečně pružně předcházet.

Jasně definovanými ISMS politikami a pravidly sladěnými napříč MČP10 bude zajištěno, že každý zaměstnanec bude v případě KBU / KBI vědět, jak se chovat a jaké aktivity a procesy v daných oblastech řešit. Při práci s IS budou mít zaměstnanci jistotu v poskytování funkcí definovaných svými rolemi, zejména pro zabezpečení spravovaných či vlastních aktiv před odcizením, a to včetně citlivých dat a údajů. Nastavená pravidla, registr rizik a práce s definovaným katalogem bezpečnostních služeb umožní pružnou reakci na hrozby, aby nebylo ohroženo poskytování byznys, aplikačních a technických služeb a neutrpěla jejich kvalita.

Cíle pro uživatele lze definovat následovně:

C-01 rozšíření povědomí o kybernetických rizicích u zaměstnanců územního samosprávného celku,

C-02 jasně definované postupy předcházení a řešení KBU / KBI,

C-03 zvýšení důvěry zaměstnanců v používané IS a tedy kvalitu služeb a dostupnost funkcí,

C-04 zlepšení ochrany spravovaných dat a informací včetně kvalifikovaného přístupu k citlivým údajům subjektů.

Opatření (legislativní požadavky) – primární efekt výstupů projektu: O-07, O-08, O-09, T-01, T-02, T-03, T-11

Přínosy na straně věcného správce (zvýšení kvality jeho výstupů, snížení pracnosti na straně jeho úředníků aj.)**:**

Přínosem pro věcného správce je v první řadě další zlepšení kvality poskytování služeb. Díky zvýšení kybernetické bezpečnosti bude značně omezeno riziko odcizení nebo kompromitace spravovaných aktiv, tedy i citlivých dat a údajů. Věcný správce bude mít jistotu, že jím garantované služby budou poskytované prostřednictvím zabezpečených IS a technologických prvků, tak jak je zasmluvněno v platných SLA. Věcný správce dále získá nové prostředky (bezpečnostní dokumentace a proškolené zaměstnance), díky kterým bude moci předcházet KBU / KBI a efektivně je řešit v případech, že nastanou.

Cíle pro věcné správce (garanty aktiv) lze definovat následovně:

C-05 poskytování bezpečných služeb, u kterých je významně sníženo riziko odcizení dat a informací,

C-06 dispozice jasně definovanými postupy a pravidly, smluvní zajištění bezpečného provozu,

C-07 dispozice zaměstnanci, kteří jsou znalí problematiky kybernetické bezpečnosti,

C-08 možnost podílet se na kvalifikovaném řízení aktiv, vést jejich evidenci a mít nad nimi možnost kontroly a rozvoje,

C-09 spolupráce s prověřenými dodavateli a partnery dodržujícími bezpečnostní politiky a přístupy,

C-10 celková kontrola nad řízením kontinuit business činností.

Opatření (legislativní požadavky) – primární efekt výstupů projektu: O-08, O-09, T-01, T-02, T-04, T-09, T-10, T-11

Přínosy pro technického správce a provozovatele služby (snížení energetické náročnosti, zjednodušení a úspora pracnosti správy systému, snížení výdajů na provoz aj.)**:**

Předcházení bezpečnostním událostem a incidentům a jejich proaktivní a efektivní řešení v první řadě přispěje k větší spolehlivosti provozovaného softwaru a technické infrastruktury.

Cíle pro technické správce a provozovatele služby jsou tyto:

C-11 bezpečně a kontrolovaně pracovat s identitami, nastavovat oprávnění,

C-12 monitorovat použití aplikací, informačních systémů, technických a komunikačních prostředků.

C-13 možnosti řídit a ověřovat práci s informacemi a daty, jejich spravování,

C-14 deklarovat a udržovat kryptografickou ochranu,

C-15 nakládat bezpečně a nerizikově s digitálními službami (v rozsahu, který se v MČP10 provozuje, bude provozovat).

C-16 efektivní a adresná podpora pro správu služeb a IS,

C-17 optimalizace pracnosti,

C-18 úspora a snížení výdajů na bezpečný provoz.

Bude tak nastavena automatizovaná, prediktivní a bezpečná operativa, která eliminuje ad-hoc manuální úkony a nárazově vynakládané (drahé) úsilí.

Opatření (legislativní požadavky) – primární efekt výstupů projektu: T-01 až T-13

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

Tabulka 8: **Vysvětlení k základním podmínkám dosažení přínosů (nutným předpokladům a rizikům dosažení celkového cíle / cílů) projektu**

Cíle projektu mohou být ohroženy spoustou různých rizik a naopak spousta okolností může přispět ke zdárnému dokončení projektu a dosažení definovaných cílů pomocí realizovaných výstupů. Jednotlivé faktory jsou zachyceny ve SWOT analýze obsažené v metamodelu.

	Užitečné	Škodlivé
Interní faktory	**Silné stránky** -- Jasně definované a nastavené bezpečnostní procesy a pravidla -- Zaměstnanci se znalostí problematiky kybernetické bezpečnosti -- Infrastruktura a SW pro monitoring a analýzu bezpečnostních událostí a incidentů -- Proaktivní kontrola vedením u poskytovaných veřejných služeb MČP10 -- Centrální správa (synergie)	**Slabé stránky** -- Na chování podle pravidel bude potřebné si navyknout -- Omezené zdroje MČP10 (pracovníci, finance, zastupitelnost) -- Malé zapojení vedení MČP10 na podpoře / rozvoji bezpečnosti a řízení rizik (aktuální efekt: safety <> security) -- Malé povědomí spoluvlastnictví aktiv - osvojit si práva a povinnosti s tím spojené -- Převažuje taktické vedení a nevnímání sady schopností organizace a potřeba jejich udržitelnosti
Externí faktory	**Příležitosti** -- Výrazně menší riziko úniků dat a informací -- Snižování nákladů na odstraňování následků KBU, KBI -- Zvětšení reputační charakteristiky MČP10 -- Digitalizace služeb, více bezpečně podporovaných kanálů komunikace se MČP10 -- Zpřehlednění agend, nastavení transparentních procesů, otevření se důvěryhodné spolupráci s partnery	**Hrozby** -- Objeví se nové typy kybernetického nebezpečí -- Zaměstnanci si nedokážou osvojit nová pravidla a procesy -- Procesy a pravidla nebudou řádně aktualizovány, aby dokázaly reagovat na nejnovější hrozby -- Pořízení nevhodných výstupů (dokumentace, nástrojů, školení) během realizace projektu, které nezajistí dosažení definovaných cílů -- Nebude doplňována legislativa dobrou smluvní základnou - prostor pro neřízenou komunikaci s ext. dodavateli služeb a řešení - pokuty, soudní spory, atp.

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

2. ARCHITEKTONICKÉ INFORMACE O PROJEKTU

2.1. Dodržení architektonických principů NA VS ČR

Tabulka 9: **Dodržení architektonických principů Národní architektury veřejné správy ČR**		
Architektonické principy byly naplněny:	Ano, použito	
Klasifikace nenaplněného principu	**Č. žádosti o výjimku**	**Vysvětlete**

Pohledy k dodržení architektonických principů a cílů:

- ***eGov Goals Catalogue***
- ***eGov Principles Catalogue***

2.2. Enterprise architektura projektu a její kontext

Tabulka 10: **Architektonický model**	
V rámci Enterprise Architektury projektu přiložte jako přílohu model exportovaný ve standardizovaném výměnném formátu The Open Group ArchiMate Model Exchange File Format	**Ano, model je přiložen jako příloha ve standardizovaném formátu**
Případně vysvětlete, proč není model přiložen ve standardizovaném formátu či není přiložen vůbec.	

2.2.1. Motivační architektura – strategie a směrování

Tabulka 11: **Vysvětlete, proč projekt realizujete v této podobě a čeho jím chcete dosáhnout.** Pro vysvětlení motivace použijte zejména pojmy z odpovídajícího modelu motivační architektury (motivátory, zainteresované osoby, cíle, principy, podmínky, architektonické požadavky)**:**

Cíle: Základním cílem, k jehož naplnění směřuje realizace projektu je zvýšení kybernetické bezpečnosti MČP10. Důvodů pro zvýšení bezpečnosti je několik. Zásadním faktorem je mít především k dispozici aktualizovanou bezpečnostní dokumentaci, která vydefinuje, jak efektivně reagovat na KBU / KBI v případě, že nastane. Dále musí být zvýšeno povědomí o kybernetických hrozbách u zaměstnanců, a to zajištěním pravidelného školení v problematice bezpečnosti. Vyškolení zaměstnanci mnohem lépe rozpoznají bezpečnostní rizika a dokážou na ně adekvátně reagovat. Viz. **Tabulka 7 v tomto dokumentu** a motivační pohledy v metamodelu.

Motivátory: Pro správu agend zaměstnanci MČP10 je rovněž důležitá eliminace rizika odcizení informací včetně citlivých dat a údajů. Motivací je zajištění stavu, kdy zaměstnanci budou pracovat s bezpečnými informačními systémy v rámci dobře definovaných a přidělovaných oprávnění, což povede k poskytování kvalitních a bezpečných služeb. Jedním z výstupů je proto pořízení monitorovacího / analytického softwaru, který zajistí sledování nežádoucích aktivit a tím prevenci před KBU / KBI.

Principy / Zásady: Jelikož MČP10 spadá mezi povinné subjekty podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti částečně, vydefinoval Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) alespoň minimální standard pravidel, která by subjekty měly dodržovat. Jedná se o dokument s názvem „Minimální bezpečnostní standard“. **Tabulka 39 v tomto dokumentu** a motivační pohledy v metamodelu. Hlediskem eGovernmentu ČR je pak zdrojem zásad a principů **Tabulka 9 zde v dokumentu** s odkazem na naplňované architektonické principy IK a NAP ČR.

Omezení: Nakonec je nutné podotknout, že aktivity subjektu směřující ke zvýšení kybernetické bezpečnosti jsou omezeny zdroji, které má k dispozici. Jedná se především o finance a lidské zdroje.

Výstupy: viz. **Tabulka 5 zde v dokumentu**

Strategické směřování: Snížení rizik kybernetických útoků, zlepšování schopností reagovat na KBI/KBU, proaktivní ochrana vlastních i spravovaných dat a informačních systémů a komunikačních prostředků (metropolitní síť), zajištění a zlepšování důvěry klientů/občanů v naše digitální služby a produkty.

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

Tabulka 12: **Nevyplnění tabulky a diagramů**	
Následující tabulku 13 a diagramy není třeba vyplňovat, pokud žadatel přiložil jako přílohu export ze svého architektonického nástroje obsahující diagramy a popis prvků.	Nevyplněno z důvodu přiložení informací jako přílohy

Tabulka 13: **Katalog prvků motivační architektury**			
ID	**Typ prvku**	**Jméno prvku**	**Popis prvku**

Pohledy „motivační architektury“:

- ***Motivační pohled - Soulad s legislativou ZKB/VKB/ZOÚ/OHA (Zásady, Výstupy, Opatření)***
- ***Motivační pohled - Výstupy, Cíle, Motivátory, Zainteresované strany***

2.2.2. Efektivita projektu – výkonnostní architektura

Tabulka 14: **Vysvětlete dopad projektu na hospodárnost, účelnost, účinnost, časovou a kvalifikační náročnost a na kvalitu služeb v organizaci (viz metodika TCO zveřejněná zde):**
Projektový záměr je od začátku plánován takovým způsobem, aby přinesl co největší efektivitu. Zajištění hospodárnosti bude dosaženo především postupem podle zákona č. 134/2016 Sb. o zadávání veřejných zakázek. Jelikož z dikce zákona plyne, že MČP10 je veřejným zadavatelem, bude nutné všechny komponenty nového řešení soutěžit v zadávacím řízení. MČP10 tedy očekává, že tím bude vybrána ta nejlepší nabídka, která zajistí náležité uspokojení potřeb při adekvátním vynaložení finančních prostředků. Realizací předmětu projektu bude zajištěna kvalita poskytovaných služeb, neboť zaměstnanci a uživatelé budou pracovat se zabezpečenými IS a technologickými prvky ekosystému, u nichž bude udrženo nízké riziko odcizení citlivých dat a prediktivní eliminace potenciálních útoků na ně vedených. Vše v souladu s uzavřenými a dodržovanými SLA vůči partnerům MČP10. Dále se od realizace očekává především kontinuální navyšování povědomí pracovníků o kybernetických hrozbách a jejich pružnou reakci v případě výskytu takové hrozby. Díky tomu MČP10 nebude muset vynakládat prostředky na externí subjekty, které mají dostatečné znalosti a dokáží takové situace externě řešit. To povede k značnému snížení vynakládaných finančních prostředků z rozpočtu MČP10. Dynamická aktualizace povědomí pracovníků o kybernetických rizicích a především zkvalitňování pravidel předcházení těmto rizikům v organizaci povede ke zvýšení prevence bezpečnostních rizik a následně ke snížení nákladů vynakládaných na jejich odstraňování. MČP10 musí mít neustále na paměti, že ani nejdokonalejší nástroje pro detekci rizik neochrání, pokud selže lidský faktor.

Tabulka 15: **Přehled požadovaných cílových parametrů SLA nových nebo měněných služeb**			
Název v rámci projektu nově zřizované nebo měněné služby	**Specifikace SLA parametru služby**	**Sjednaná mezní hodnota SLA parametru**	**Sjednaný způsob měření hodnoty SLA**
Nerelevantní, nejde o externalizované bezpečnostní služby (mimo MČP10), které by byly měněny nebo nově zřizovány. Konzultováno s OHA DIA.			

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

2.2.3. Byznys architektura

Tabulka 16: **Nevyplnění tabulky a diagramů**	
Následující tabulku 17 a diagramy není třeba vyplňovat, pokud žadatel přiložil jako přílohu export ze svého architektonického nástroje obsahující diagramy a popis prvků.	Nevyplněno z důvodu přiložení informací jako přílohy

Tabulka 17: **Katalog prvků byznys architektury**			
ID	**Typ prvku**	**Jméno prvku**	**Popis prvku**

Tabulka 18: **Využití front-office rozhraní předmětem projektu**			
Rozhraní	**Využití**		**Popis využití rozhraní v projektu**
Asistovaná přepážka			
Umožnění asistovaného vyřízení podání či jiné služby v rámci projektu	Nerelevantní		Projekt řeší kybernetickou bezpečnost. Otázka využití rozhraní front-office (tj. rozhraní, skrze které dochází ke styku s klientem veřejné správy) předmětem projektu je tudíž nerelevantní.
	Č. žádosti o výjimku:		
Umožnění vyřízení služby na Kontaktním místě veřejné správy (Czech POINT)	Nerelevantní		
	Č. žádosti o výjimku:		
Webový portál			
Identifikace úředních osob vstupujících do procesu je řešena v souladu s CAAIS (dříve JIP/KAAS)	Nerelevantní		
	Č. žádosti o výjimku:		
Identifikace osob vstupujících do procesu je řešena v souladu se zákonem č. 250/2017 Sb., o elektronické identifikaci	Nerelevantní		
	Č. žádosti o výjimku:		
Datová zpráva (ISDS)			
Využití Datových schránek pro účely doručování od OVM soukromoprávním subjektům a mezi OVM navzájem	Nerelevantní		
	Č. žádosti o výjimku:		
Využití datových schránek pro účely dodávání mezi soukromoprávními subjekty navzájem	Nerelevantní		
	Č. žádosti o výjimku:		
Využití Informačního systému datových schránek pro účely příjmu úkonů učiněných soukromoprávním subjektem vůči OVM (např. podání)	Nerelevantní		
	Č. žádosti o výjimku:		
Elektronicky podepsaný dokument do e-Podatelny	Nerelevantní		
Nepodepsaný dokument do e-Podatelny	Nerelevantní		
Listinnou cestou do podatelny	Nerelevantní		

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

Tabulka 19: **Identifikace, autentizace a autorizace subjektů/uživatelů v jejich rolích**			
Služba využívající identifikaci, autentizaci a autorizaci	**Vysvětlete způsob identifikace a autentizace do služby**	**Použitý prostředek (Pokud není určený LoA[5] v NIA) a druh autentizace**	**Vysvětlete autorizaci ve službě (přidělení role, mandáty, zastupování, atd.)**
ASDP	uživatelské jméno, heslo (interní databáze systému)	LoA 1 – přístupové údaje	Přidělování role v systému – řídí garant systému
Call 250V (WebCall)	PIN (interní databáze systému)	LoA 1 – PIN	Přidělování role v systému – role dle funkčního místa
CIS – ZPS	uživatelské jméno, heslo (interní databáze systému)	LoA 1 – přístupové údaje	Přidělování role v systému – řídí garant systému
CDSw (Dopravní značení, CityInfo, Nehodovost, UCHO, Zeleň, ZUK)	uživatelské jméno, heslo (SSO AD)	LoA 1 – účet v AD	Přidělování role v systému – schvaluje garant systému
Czech POINT (JIP/KAAS; CAAIS; DS; základní registry a evidence)	uživatelské jméno, heslo + certifikát (interní databáze systému)	LoA 2 – OTP / LoA 3 – certifikáty certifikačních autorit	Přidělování role v systému – role dle funkčního místa + schvalování garantem systému
ELO	uživatelské jméno, heslo (interní databáze systému)	LoA 1 – přístupové údaje	Přidělování role v systému – schvaluje garant systému
e-Spis	uživatelské jméno, heslo (SSO AD)	LoA 1 – účet v AD	Přidělování role v systému – role dle funkčního místa
GINIS (UCR, ROZ, MAJ, KDF, KOF, POK, POU, SML, OBJ, DDP, BUC, ADM, BAR, INU, VYK, FUC, PPD, EMA)	uživatelské jméno, heslo (interní databáze systému)	LoA 1 – přístupové údaje	Přidělování role v systému – role dle funkčního místa + schvalování garantem systému
iDES	uživatelské jméno, heslo (interní databáze systému)	LoA 1 – přístupové údaje	Přidělování role v systému – schvaluje garant systému
Intranet	uživatelské jméno, heslo (SSO AD)	LoA 1 – účet v AD	Přidělování role v systému – role dle funkčního místa
Kanboard	uživatelské jméno, heslo (interní databáze systému)	LoA 1 – přístupové údaje	Přidělování role v systému – řídí garant systému
MISYS	uživatelské jméno, heslo (SSO AD)	LoA 1 – účet v AD	Role dle AD skupiny – schvaluje garant systému
OKbase (Docházka; Personalistika a mzdy; Vzdělávání)	uživatelské jméno, heslo (SSO AD)	LoA 1 – účet v AD	Přidělování role v systému – role dle funkčního místa + schvalování garantem systému
PROXIO	uživatelské jméno, heslo (SSO AD)	LoA 1 – účet v AD	Přidělování role v systému – role dle funkčního místa + schvalování garantem systému
RŽP	certifikát	LoA 3 – certifikát MPO	Přidělování role v systému – řídí garant systému
VITA (Stavební úřad, Vodoprávní úřad, Přestupky)	uživatelské jméno, heslo (SSO AD)	LoA 1 – účet v AD	Přidělování role v systému – role dle funkčního místa + schvalování garantem systému
Webové stránky P10	uživatelské jméno, heslo (interní databáze systému)	LoA 1 – přístupové údaje	Přidělování role v systému – řídí garant systému
Systém elektronické pošty – Exchange	uživatelské jméno, heslo + MFA (SSO AD)	LoA 2 – OTP / LoA 3 – biometrie v authenticatoru	Nerelevantní

Modely byznys architektury (výkonu veřejné správy) – pohled činnostních funkcí, služeb veřejné správy a další

- **Business pohled - Aplikační služby vs. Business role**
- **Business pohled - Procesní kooperace KBU, KBI**
- **Business pohled - Realizace výstupů**

Tabulka 20: **Vysvětlení kontextu byznys architektury úřadu**
a) jaké k projektu existují či vznikají duplicity a proč?
V projektu neexistují ani nevznikají duplicity, multiplicity jsou naopak redukovány.

[5] LoA (Level of Assurance) – je úroveň záruky, kterou splňuje kvalifikovaný systém či prostředek pro elektronickou identifikaci podle prováděcího nařízení Komise (EU) 2015/1502. Může být nízká, značná či vysoká (1 - low, 2 - substantial, 3 - high).

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

Tabulka 20: **Vysvětlení kontextu byznys architektury úřadu**
b) jsou využity všechny sdílené služby?
V možné odpovídající míře ano.
Vysvětlení byznys architektury projektu:
Business pohled - Realizace výstupů: • Primárním cílem je zajištění, udržení a kontinuální navyšování kybernetické bezpečnosti MČP10 a tím snížení dopadů kybernetických rizik. Legislativa ČR / EU v této oblasti dává jasná kritéria opatření, která je potřeba v MČP10 udržovat. • Nejdůležitějšími aktéry jsou v tomto ohledu v rámci Povinné osoby: Výbor KB, skládající se z Manažera KB, Architekta KB, Auditora KB, dále zástupců vrcholového vedení (např. člen představenstva, popřípadě ředitel společnosti / úřadu). o **Výbor KB** bude mít odpovědnost za řízení a rozvoj kybernetické bezpečnosti v organizaci. o **Manažer KB** je zodpovědný za nastavování systému řízení bezpečnosti informací, především za určení aktiv a jejich zranitelnosti, nastavování bezpečnostních opatření, řízení rizik a jejich kontrolu. Nastavení bezpečnostních opatření v organizaci je nutné pravidelně vyhodnocovat. Pravidelné vyhodnocování bude zajištěno prostřednictvím auditování kybernetické bezpečnosti nezávislým auditorem. o **Auditor KB** je osoba s příslušnou odborností a posuzuje soulad opatření nastavených v organizaci s právními předpisy a s nejlepší praxí v oblasti kybernetické bezpečnosti. o Za návrh bezpečnostních opatření a jejich implementaci je odpovědný **Architekt KB**. o Za zajištění rozvoje, použití a bezpečnosti aktiva je zodpovědný příslušný **Garant aktiva** (Věcný správce). o Specifická aktiva jako jsou PII, tj. osobní údaje a řízení nakládání s nimi při jejich zpracování má ve své gesci **Pověřenec ochrany / zpracování osobních údajů** (DPO / DOO). Business pohled - Procesní kooperace: Koncept zpracování KBU / KBI zachycuje jejich procesy detekce, vyhodnocování a hlášení. Business pohled – Aplikační služby vs. Business role: Primární fokus je zde na vazby mezi klíčovými business rolemi a aktéry a odpovídajícími aplikačními službami zapouzdřujícími aplikační funkce.

2.2.4. Architektura informačních systémů (aplikací a dat)

2.2.4.1. Architektura informačních systémů – část: Aplikační architektura

Tabulka 21: **Nevyplnění tabulky a diagramů**	
Následující tabulku 22 a diagramy není třeba vyplňovat, pokud žadatel přiložil jako přílohu export ze svého architektonického nástroje obsahující diagramy a popis prvků.	Nevyplněno z důvodu přiložení informací jako přílohy

Tabulka 22: **Katalog všech aplikačních komponent řešení a klíčových aplikačních funkcí**			
ID	**Typ prvku**	**Jméno prvku**	**Popis prvku**

Modely aplikační architektury – pohled struktury aplikací, komunikace aplikací:

- **Aplikační pohled - Kooperace (služby, funkce, komponenty)**
- **Aplikační pohled - Struktura komponent**

Tabulka 23: **Vysvětlení v kontextu aplikační architektury úřadu**
a) jaké k projektu existují či vznikají duplicity?
V projektu neexistují ani nevznikají duplicity, multiplicity jsou naopak redukovány.
b) proč a jsou využity všechny sdílené služby?
V možné odpovídající míře ano.
Vysvětlení aplikační architektury projektu:
Aplikační pohled – struktura: Pohled na strukturu aplikací zachycuje především jednotlivé součásti aplikačního portfolia MČP10 (komponenty a data). Tyto aplikace pak slouží výhradně k výkonu agend organizace (ať už v samostatné nebo přenesené působnosti), které směřují především vně ke klientům veřejné správy. Z pohledu organizace

Tabulka 23: **Vysvětlení v kontextu aplikační architektury úřadu**
jsou však důležité i další aplikace, které zajišťují řádný vnitřní chod jejího informačního systému a bezpečnost. V modelu jsou proto komponenty, které se především podílejí na zajištění bezpečnosti barevně odlišeny. Aplikační pohled – kooperace: Pohled kooperace aplikací pak zachycuje především funkcionalitu jednotlivých komponent IS a externalizaci služeb, které jsou poskytovány vně na základě výkonu funkcí organizace, klientům veřejné správy. Služby a funkce, které se však podílejí na zajištění kybernetické bezpečnosti organizace směřují hlavně dovnitř a jsou barevně odlišeny. Aplikační architektura tak názorně ukazuje, že pro MČP10 není důležité jen zajišťování služeb směřujících vně, ale rovněž ochrana bezpečnosti vlastního IS proti kybernetickým hrozbám.

2.2.4.2. Architektura informačních systémů – část: Datová architektura

Tabulka 24: **Katalog datových objektů a subjektů:**			
Objekt nebo subjekt, který je předmětem evidence	**Vysvětlení objektu nebo subjektu**	**Označení objektu nebo subjektu dle Agend VS**	**Je objekt čerpán nebo poskytován jiným subjektům?**
Záznamy logů	Jedná se o data, která zachycují přístup a chování uživatelů v aplikacích MČP10.		Není poskytován ani čerpán
Kmen identitních dat	Identity uživatelů aplikací MČP10 a přístupová práva. Zajišťuje přístup pracovníků MČP10 k aplikacím a práci v nich.		Není poskytován ani čerpán
Bezpečnostní hrozby / Bezpečnostní události	Hrozba představující riziko pro informační systém MČP10.		Není poskytován ani čerpán
Aktiva / Modely	Jedná se o data zachycující evidenci IT aktiv či arch. konceptů.		Není poskytován ani čerpán
Analýzy / Posouzení	Jedná se o data pro řízení rizik nebo bezpečnostní auditní nálezy.		Není poskytován ani čerpán
Pravidla / Opatření	Jedná se o data s pravidly pro KB nebo kontrolní opatření k zajištění KB/PII.		Není poskytován ani čerpán

Tabulka 25: **Využití datového fondu základních registrů a dalších agend**			
Název	**Použito**		**Vysvětlení**
Základní registry			
Způsob vedení datového kmene fyzických osob	Nerelevantní		Projekt se týká kybernetické bezpečnosti. Neřeší datový fond. Vedení datového kmene je v tomto případě nerelevantní.
Čtení údajů ROB	Nerelevantní		
	Č. žádosti o výjimku:		
Editace údajů ROB	Nerelevantní		
	Č. žádosti o výjimku:		
Čtení údajů ROS	Nerelevantní		
	Č. žádosti o výjimku:		
Editace údajů ROS	Nerelevantní		
	Č. žádosti o výjimku:		

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

Tabulka 25: **Využití datového fondu základních registrů a dalších agend**			
Název	**Použito**		**Vysvětlení**
Čtení údajů RÚIAN	Nerelevantní		
	Č. žádosti o výjimku:		
Editace údajů RÚIAN	Nerelevantní		
	Č. žádosti o výjimku:		
Čtení údajů RPP	Nerelevantní		
	Č. žádosti o výjimku:		
Editace údajů RPP	Nerelevantní		
	Č. žádosti o výjimku:		
Evidujeme subjekty nebo objekty, které nejsou v základních registrech	Ne		
Využití údajů publikovaných prostřednictvím kompozitních služeb editorů Základních registrů			
Evidence obyvatel (ISEO)	Nerelevantní		
	Č. žádosti o výjimku:		
Cizinecký informační systém (CIS)	Nerelevantní		
	Č. žádosti o výjimku:		
Evidence občanských průkazů (AISEOP)	Nerelevantní		
	Č. žádosti o výjimku:		
Evidence cestovních dokladů (AISECD)	Nerelevantní		
	Č. žádosti o výjimku:		
Informační systém sdílené služby (ISSS dříve jako eGSB)			
Čerpání dat přes ISSS	Nerelevantní		
	Č. žádosti o výjimku:		
Publikování vlastních dat přes ISSS	Nerelevantní		
	Č. žádosti o výjimku:		
Komunikace mimo propojený datový fond			
Využívání vlastních proprietárních rozhraní	Nerelevantní		
	Č. žádosti o výjimku:		
Využívání Czech POINT pro přístup nebo editaci údajů PPDF	Ne		

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

Tabulka 26: **Způsob zajištění vedení datového kmene**			
Požadavek	**Použito**		**Vysvětlení**
Zajištění přístupu k datům pro správce předmětu projektu			
Budete mít zajištěn přístup k veškerým datům vedeným v databázích dotčených předmětem projektu ve strojově čitelném a otevřeném formátu?	Nerelevantní		Projekt se týká kybernetické bezpečnosti, neřeší práci s daty.
	Č. žádosti o výjimku:		
Budete mít výše popsaný přístup k datům zajištěn bez dodatečných finančních nákladů?	Nerelevantní		
	Č. žádosti o výjimku:		
Budete moci se zpřístupněnými daty libovolně nakládat?	Nerelevantní		
	Č. žádosti o výjimku:		
Publikace výstupů ve formátu otevřených dat			
Budou data vedená v databázích dotčených předmětem projektu zveřejňována jako otevřená data?	Nerelevantní		Projektem není řešeno publikování otevřených dat.
	Č. žádosti o výjimku:		
Jaké datové oblasti plánujete zveřejňovat jako otevřená data, kdy a na jakém stupni otevřenosti?			

Tabulka 27: **Nakládání s osobními a citlivými údaji**			
Způsoby identifikace subjektů (FO, PO) v informačním systému	AIFO	Ne	*Projekt se týká kybernetické bezpečnosti, neřeší nakládání s osobními a citlivými údaji.*
	IČO	Ne	
	Rodné číslo	Ne	
	Vlastní klientský identifikátor	Ne	
	Jiný identifikátor	Ne	
Předpokládaný počet subjektů údajů dotčených zpracováním osobních údajů v systému (orientační počet osob, jejichž údaje budou v systému zpracovávány)			

Tabulka 28: **Vysvětlení v kontextu datové architektury úřadu**
a) jaké k projektu existují či vznikají duplicity?
V projektu neexistují ani nevznikají duplicity, multiplicity jsou naopak redukovány.
b) jsou využity všechny sdílené služby?
V možné odpovídající míře ano.
Vysvětlení datové architektury projektu:
Pohled na datovou architekturu opět ukazuje datové objekty, které mají největší význam právě pro oblast zajišťování kybernetické bezpečnosti (logy, identitní data, bezpečnostní hrozby, evidence aktiv). Data jsou nezbytná především za účelem prevence a včasné detekce bezpečnostních rizik. Samotná data však sama o sobě mnoho nevypoví, proto je třeba je sledovat a vyhodnocovat. Na aplikační vrstvě je přesně toto úkolem komponenty SIEM/SOC, dále také úložiště aktiv a konceptů/modelů, aplikační komponenty pro práci s daty důležitými pro analýzy v oblasti GRC.

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

2.2.5. Technologická architektura – vrstva IT technologie (HW a SW)

Tabulka 29: **Nevyplnění tabulky a diagramů**	
Následující tabulku 30 a diagramy není třeba vyplňovat, pokud žadatel přiložil jako přílohu export ze svého architektonického nástroje obsahující diagramy a popis prvků.	Nevyplněno z důvodu přiložení informací jako přílohy

Tabulka 30: **Katalog uzlů a klíčových funkcí nebo služeb**

ID	Typ prvku	Jméno prvku	Popis prvku

Diagram technologické architektury – pohled struktury IT technologické architektury

Tabulka 31**: Cloud Computing**

Požadavek	Odpověď	Vysvětlení
Bude pro řešení využito služeb cloud computingu dle výsledku ekonomické výhodnosti provozu?	Ne	
Uveďte odkaz na poptávku, nabídku nebo využívání z katalogu cloud computingu		
Jak dodržujete vyhlášku č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu, pokud cloud computing využíváte pro navrhované řešní?		Nerelevantní

Tabulka 32: **Vysvětlení v kontextu technologické architektury úřadu**
a) jaké k funkčnímu celku existují či vznikají duplicity?
V projektu neexistují ani nevznikají duplicity, multiplicity jsou naopak redukovány.
b) jsou využity všechny sdílené služby?
V možné odpovídající míře ano.
Vysvětlení technologické architektury projektu:
Technologický pohled – Užití: Technologická architektura je reprezentována technologickými prostředky, na kterých jsou MČP10 provozovány její aplikace. Jde především o prvky technologické architektury (vrstvy), tj. servery a další zařízení. Jelikož je předmět projektu orientován na zvýšení kybernetické bezpečnosti, je v modelu věnována pozornost především souvisejícím službám a zařízením, jako jsou firewally, sondy, zálohovací zařízení a monitorovací služby (viz barevné rozlišení).

2.2.6. Technologická architektura – vrstva komunikační infrastruktury

Tabulka 33: **Nevyplnění tabulky a diagramů**	
Následující tabulku 33 a diagramy není třeba vyplňovat, pokud žadatel přiložil jako přílohu export ze svého architektonického nástroje obsahující diagramy a popis prvků.	Nevyplněno z důvodu přiložení informací jako přílohy

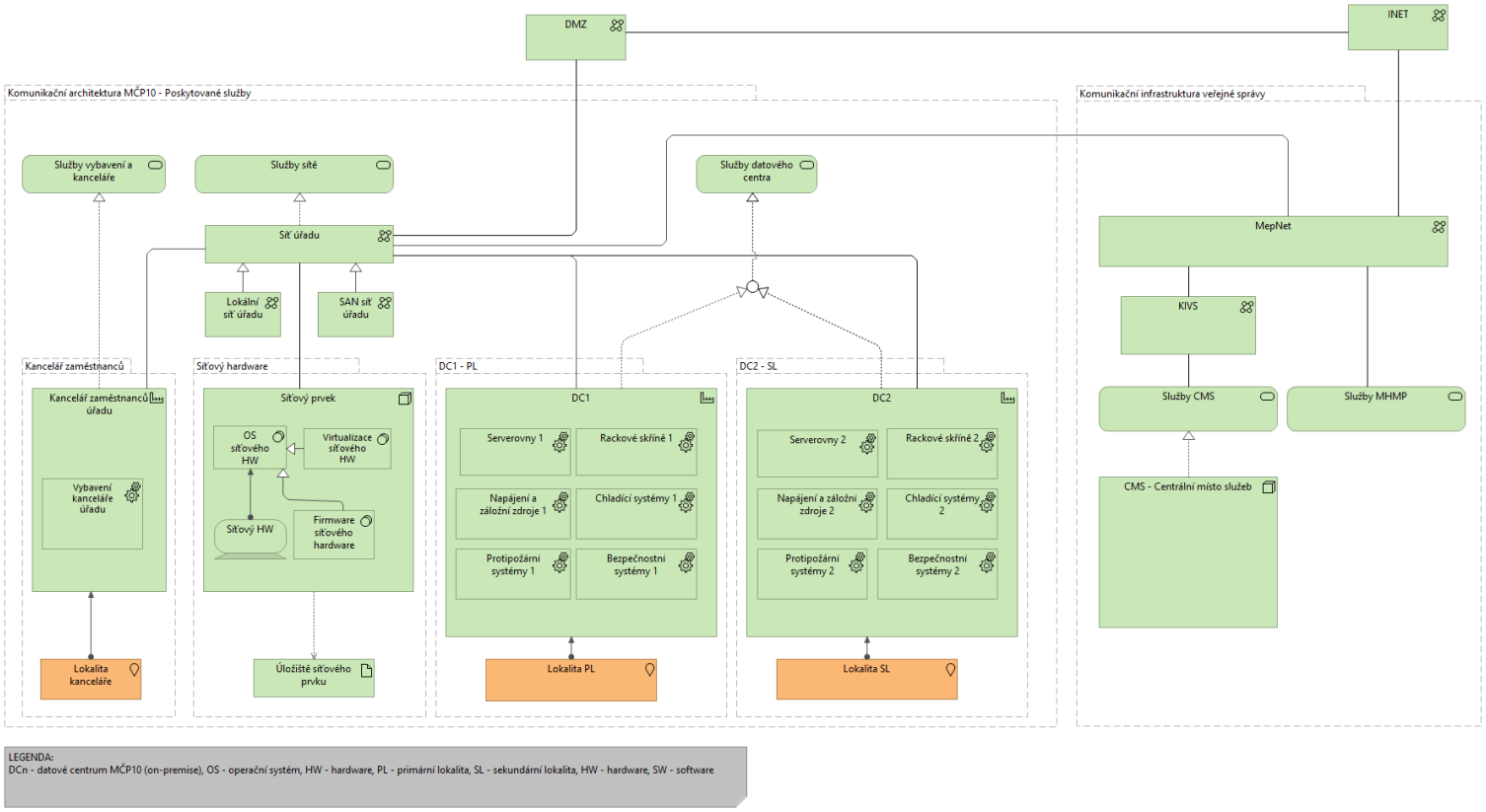
Tabulka 34: **Katalog infrastrukturních komunikačních funkcí, sítí, cest a klíčových služeb**

ID	Typ prvku	Jméno prvku	Popis prvku

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

Modely technologické architektury – pohled struktury komunikační infrastruktury:

- **Technicko-Fyzický pohled – Multivrstvy**



Tabulka 35: **Využití sdílených služeb komunikační infrastruktury**			
Název	**Popis**	**Použito**	**Č. žádosti o výjimku**
CMS	Pro publikaci či čerpání služeb v tomto projektu je využito Centrální místo služeb	Nerelevantní	
KIVS	Jakým způsobem přistupujete do CMS druhé generace?	KIVS	
Internet	Využíváte vlastní připojení do veřejného internetu?	Ano	

Tabulka 36: **Vysvětlení v kontextu architektury komunikační infrastruktury úřadu**
a) jaké k projektu existují či vznikají duplicity a proč?
V projektu neexistují ani nevznikají duplicity, multiplicity jsou naopak redukovány.
b) jsou využity všechny sdílené služby?
V možné odpovídající míře ano
Vysvětlení architektury komunikační infrastruktury projektu:
Technicko-Fyzický pohled – Multivrstvy: Komunikační vrstva zajišťuje v rámci technologické architektury tok dat mezi jednotlivými technologickými prvky podporujícími IS MČP10 a dále zajišťuje komunikaci s vnějším světem. Tyto úkoly komunikační vrstvy jsou zajišťovány prostřednictvím sítí poskytujících síťové služby.

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

2.2.7. Bezpečnostní architektura

Tabulka 37: **Katalog bezpečnostní architektury projektu**		
Dotčený nebo bezpečnostní prvek	**Hrozba / riziko**	**Vysvětlení způsobu zmírnění hrozby / rizika prvkem architektury včetně technických a organizačních opatření**

Tabulka 37b: **Nevyplnění tabulky a diagramů**	
Předcházející tabulku 37a a diagramy není třeba vyplňovat, pokud žadatel přiložil jako přílohu export ze svého architektonického nástroje obsahující diagramy a popis prvků.	Nevyplněno z důvodu přiložení informací jako přílohy

Tabulka 38: **Dopady narušení bezpečnosti informací v systému**	
Možné dopady v případě narušení dostupnosti	V případě narušení dostupnosti je ohrožen výkon řady agend (funkcí), které MČP10 vykonává. Narušením dostupnosti služeb, potažmo nedostupností funkcí (agend) jako takových, by tak bylo ohroženo poskytování produktů poptávajícím stranám (fyzickým či právnickým osobám). Výčet agend, které by byly narušeny (https://rpp-ais.egon.gov.cz/gen/agendy-detail/), se obvykle liší i v závislosti na tom, jaké služby jsou koncepčně řešeny informačními systémy MČP10 a jaké mají výkonnostní a bezpečnostní charakteristiky, které musí MČP10 naplňovat.
Možné dopady v případě narušení důvěrnosti	Narušení důvěrnosti a ohrožení dat informačních systémů MČP10 se bude lišit v závislosti na tom, jak velký datový kmen konkrétní orgán zpracovává. Některé MČP jsou, co do obyvatelstva, početnější, jiná méně. Ohrožení dat a narušení jejich důvěrnosti však v každém případě může přivodit újmu na právech postižených subjektů a dále nedůvěru k příslušným samosprávným orgánům. U MČP10 je možné se bavit o ohrožení dat v řádu statisíců subjektů.
Možné dopady v případě narušení integrity	Narušení integrity informací může zapříčinit práci s nesprávnými informacemi a poškodit práva oprávněných subjektů. Riziko narušení integrity MČP10 se podstatně sníží pořízením komponenty log managementu a SIEM/SOC/GRC pro zaznamenávání nestandardního chování a vyhodnocování rizik.
Je v rámci Vaší organizace určen jakýkoliv prvek kritické infrastruktury?	Ne
Jste seznámeni a dodržujete Bezpečnostní strategii ČR 2023 dle usnesení vlády č. 478 ze dne 28. 06. 2023 včetně např. riziky využívání produktů čínských výrobců?	Ano
Jak naplňujete doporučení v oblasti kryptografických prostředků v3.0 https://www.nukib.cz/cs/infoservis/doporuceni/1988-doporuceni-v-oblasti-kryptografickych-prostredku-verze-3-0/?	Doporučení jsou aplikována v potřebném rozsahu pro jednotlivé prvky zabezpečené architektury. Pro vývoj problematiky jsou nadále sledována a posuzována doporučení NÚKIB před jejich nasazením v MČP10.
Případně specifikujte ty určené prvky KI, jejichž činnost významně nebo zcela ovlivňuje tento posuzovaný informační systém:	

Tabulka 39: **Bezpečnostní opatření a zohlednění principu „security by design“**		
Bezpečnostní opatření dle Minimálního bezpečnostního standardu NÚKIB (dále jen „MBS“)	**Odpověď**	**Popis realizace, případně odůvodnění nezavedení**
Organizační opatření		
Plán zavádění bezpečnostních opatření (kapitola 2.1 MBS)	Ano	Zajištěno. MČP10 s vytvořením takového plánu počítá. **(O-01, O-13)**
Klasifikace a ochrana informací (kapitola 3 MBS)	Ano	Zajištěno. Definováno v rámci byznys architektury. **(O-06, T-11)**

Řízení dodavatelů (kapitola 4 MBS)	Ano	Zajištěno. Definováno v rámci byznys architektury. **(O-03, O-05, O-09, O-07, O-10)**
Řízení lidských zdrojů (kapitola 5 MBS)	Ano	Zajištěno. Definováno v rámci byznys architektury. **(O-07)**
Řízení změn (kapitola 6 MBS)	Ano	Zajištěno. Definováno v rámci byznys architektury. **(O-10, O-06, O-04)**
Řízení kontinuity činností (kapitola 7 MBS)	Ano	Zajištěno. Definováno v rámci byznys architektury. **(O-12, O-08)**
Audit kybernetické bezpečnosti (kapitola 8 MBS)	Ano	Zajištěno. Definováno v rámci byznys architektury. **(O-13)**
Další opatření	Ano	Počítá se s pravidelným školením pracovníků za účelem zvýšení jejich povědomí o kybernetických hrozbách a rizicích. Dále se počítá s pořízením komponent (Log management, SIEM, EAM, GRC) pro komplexní vyhodnocování bezpečnostních rizik. **(O-07, O-02, T-06, O-06, T-06, T-07, T-08)**
Technická opatření		
Fyzická bezpečnost (kapitola 9 MBS)	Ano	Zajištěno. MČP10 disponuje kamerovým systémem za účelem monitorování prostorů úřadu a místností se servery. Prostor úřadu je hlídán bezpečnostní agenturou. **(T-01)**
Řízení přístupů (kapitola 10 MBS)	Ano	Zajištěno. Přístup do místností se servery a infrastrukturou je chráněn čtečkou čipových karet. Vstup je povolen pouze oprávněným držitelům. **(T-09)**
Ochrana před škodlivým kódem (kapitola 11 MBS)	Ano	Zajištěno. Aplikace a infrastruktura jsou chráněny kvalitním antivirovým softwarem. **(T-05)**
Řešení kyberbezpečnostních událostí a incidentů (kapitola 12 MBS)	Ano	Zajištěno. Definování procesu pro řešení KBU / KBI je jedním z výstupů projektu. Definováno na byznys vrstvě. **(T-07, T-08)**
Aplikační bezpečnost (kapitola 13 MBS)	Ano	Zajištěno. . Počítá se s nasazením SIEM a komponenty pro správu identit a přístupů. Předpokládá se vyhodnocování logů s ohledem na zajištění bezpečnosti před možnými kybernetickými hrozbami. **(T-09, T-06, T-07, T-04, T-03)**
Kryptografické prostředky (kapitola 14 MBS)	Ano	Zajištěno. Počítá se s rozvojem a řízením použití kryptografických prostředků. **(T-10)**
Zajišťování úrovně dostupnosti informací (kapitola 15 MBS)	Ano	Zajištěno v návaznosti na Business continuity plan. **(T-11, O-12)**
Požadavky v oblasti cloudových služeb (kapitola 16 MBS)	Ano	Záleží na konkrétním řešení. **(T-13)**
Řízení výjimek běhu, chyb a hlášení (kapitola 17.1 MBS)	Ano	Zajištěno. Logovací komponenta zachytí všechny nestandardní situace, které budou následně vyhodnocovány s využitím SIEM [NOC+SOC]. **(T-02, T-06)**
Ochrana webových aplikací (kapitola 17.2 MBS)	Ano	Zajištěno. Komunikace s aplikacemi pomocí kanálu zabezpečeného s využitím technologie SSL. **(T-09)**
Zabezpečení komunikace s externími systémy (kapitola 17.4 MBS)	Ano	Zajištěno. S externími systémy bude komunikováno výhradně s využitím zabezpečené komunikační infrastruktury. **(T-02, T-10)**
Další opatření	Ano	Mezi další opatření, která budou předmětem projektu zavedena, patří pravidelná školení zaměstnanců za účelem získání povědomí o kybernetických hrozbách. Dále je počítáno s nastavením bezpečnostních pravidel, procesů a s jejich důsledným uplatňováním v praxi. **(O-01, O-02, O-03, O-04, O-07)**

Tabulka 40: **Vysvětlení bezpečnostní architektury projektu**

Zvýšení bezpečnosti (konkrétně kybernetické bezpečnosti) je hlavním cílem, který realizace projektu sleduje. Bezpečnostní architektura se neomezuje pouze na některou z vrstev (aplikační, technologická), se kterou bývá kybernetická bezpečnost tradičně spojována, nicméně prolíná se všemi vrstvami architektury včetně byznysové. Nejnovější nástroje pro detekci bezpečnostních hrozeb totiž nestačí jen svojí základní funkcionalitou, pokud nejsou řádně nastavena pravidla pro detekci a hlášení KBU a KBI a také pravidla, která je nutná dodržovat pracovníky MČP10 za účelem předcházení bezpečnostním hrozbám. Při návrhu bezpečnostní architektury tak nelze žádnou vrstvu ostatních architektur opomenout. Jde o velmi důležitou informaci, ke které by při návrhu řešení k posílení kybernetické bezpečnosti měla MČP10 vždy přihlížet.

2.2.8. Shoda s pravidly, standardizace a dlouhodobá udržitelnost

Tabulka 41: **Uveďte, které licence standardizovaných SW produktů nebo HW produktů budete pořizovat formou centrálních rámcových smluv zajištěných Ministerstvem vnitra. Pokud tuto formu nevyužijete, vysvětlete proč:**

V plánu je pořídit specializované nástroje, které není možné pořídit prostřednictvím centrálních rámcových smluv Ministerstva vnitra.

Rámec	Odpověď	Vysvětlení důvodů nepoužití
Centrální nákup produktů Cisco Systems	Ne	Důvod nevyužití uveden v záhlaví.
Centrální nákup produktů IBM	Ne	Důvod nevyužití uveden v záhlaví.

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

Tabulka 41: **Uveďte, které licence standardizovaných SW produktů nebo HW produktů budete pořizovat formou centrálních rámcových smluv zajištěných Ministerstvem vnitra. Pokud tuto formu nevyužijete, vysvětlete proč:**		
Centrální nákup produktů Microsoft	Ne	Důvod nevyužití uveden v záhlaví.
Centrální nákup produktů Oracle	Ne	Důvod nevyužití uveden v záhlaví.
Centrální nákup produktů VMware	Ne	Důvod nevyužití uveden v záhlaví.
Centrální nákup CITRIX	Ne	Důvod nevyužití uveden v záhlaví.
Centrální nákup ICT komodit	Ne	Důvod nevyužití uveden v záhlaví.
Centrální soutěžení KIVS	Ne	Důvod nevyužití uveden v záhlaví.

Tabulka 42: **UX/UI uživatelský zážitek a uživatelské rozhraní**			
Požadavek	**Odpověď**	**Číslo žádosti o výjimku**	**Vysvětlení**
Primární výzkum (úvodní analýza)			
Znáte svoji cílovou skupinu a její specifika?	Ne		Jde o projekt řešící kybernetickou bezpečnost.
Plánujete rešerši obdobných již implementovaných řešení?	Ne		Jde o projekt řešící kybernetickou bezpečnost.
U redesignu - budete identifikovat pain pointy?	Ne		Jde o projekt řešící kybernetickou bezpečnost.
U redesignu - máte k dispozici měření a výstupy z analytických nástrojů?	Ne		Jde o projekt řešící kybernetickou bezpečnost.
Design			
Plánujete mapování procesů a uživatelských cest?	Nerelevantní		Jde o projekt řešící kybernetickou bezpečnost.
Plánujete navržení / optimalizaci informační architektury?	Nerelevantní		Jde o projekt řešící kybernetickou bezpečnost.
Víte, pro jaká zařízení budete řešení designovat a počítáte s responzivním designem?	Ne		Jde o projekt řešící kybernetickou bezpečnost.
Bude projekt využívat design systém gov.cz?	Nerelevantní		Jde o projekt řešící kybernetickou bezpečnost.
Ověření funkčnosti designu			
Budete dělat wireframes k ověření konceptu?	Ne		Jde o projekt řešící kybernetickou bezpečnost.
Budete dělat mid-high fidelity prototypy pro testování s uživateli?	Ne		Jde o projekt řešící kybernetickou bezpečnost.
Před spuštěním projektu			
Bude projekt zahrnovat kontrolu přístupnosti?	Nerelevantní		Jde o projekt řešící kybernetickou bezpečnost.
Bude projekt navázán na optimalizaci pro vyhledávače (SEO)?	Nerelevantní		Jde o projekt řešící kybernetickou bezpečnost.
Jaké analytické nástroje budete využívat pro měření úspěchu projektu?	Nerelevantní		Jde o projekt řešící kybernetickou bezpečnost.
Jakým způsobem budete sbírat zpětnou vazbu od uživatelů?	Nerelevantní		Jde o projekt řešící kybernetickou bezpečnost.
Jak budete zpracovávat vyplývající změny?	Nerelevantní		Jde o projekt řešící kybernetickou bezpečnost.

Tabulka 43: **Shoda se strategickými dokumenty**			
Požadavek	**Odpověď**	**Číslo žádosti o výjimku**	**Vysvětlení**
Je řešení v souladu s Informační koncepcí úřadu?	Ano		Projekt není v rozporu s aktuální vizí hl. m. Prahy a v současné době připravovanými celoměstskými projekty a nevytváří k nim duplicitu (viz usnesení v Zápisu z ŘV CMK v příloze).
Je řešení v souladu s Informační koncepcí ČR a cíli či principy Digitálního Česka?	Ano		

Tabulka 44: **Legislativní update**	
Bude podpora zahrnovat rovněž udržování řešení v souladu s novými právními předpisy (tzv. legislativní update)**?** **Vysvětlete, v jakém rozsahu:**	**Jakým způsobem bude legislativní update hrazen?**
Případný legislativní update je koncipován jako součást smluv o provozu a podpoře.	Součást smlouvy o provozu a podpoře

Tabulka 45: **Jak je zajištěno řízené ukončení životnosti jednotlivých výstupů projektu a případný přechod na další řešení, či případná výměna dodavatele nad stejným řešením** (tzv. Exit strategie):
Smlouva s dodavatelem bude obsahovat příslušná ustanovení umožňující, aby v případě potřeby mohl zadavatel smlouvu vypovědět a soutěžit dodavatele nového. Součástí smlouvy bude rovněž povinnost stávajícího dodavatele převést data a veškerou administrativu související s provozem k dodavateli novému.

Tabulka 46: **Vysvětlení standardizace a udržitelnosti architektury projektu**
Předmět projektu bude dodržovat všechny požadavky aktuálně platné legislativy. Počítáno je také s úpravami v případě legislativních změn (update součástí smlouvy o provozu a podpoře). Dále je počítáno s využitím nejlepších praktik (best practices) v oblasti kybernetické bezpečnosti a úzká spolupráce s příslušnými autoritami, jako je například NÚKIB. Pro zajištění udržitelnosti kybernetické bezpečnosti budou prováděny pravidelné audity, jak zachycuje vrstva business architektury.

2.3. Kontrola shody architektury řešení projektu s požadavky Národního architektonického plánu

Tabulka 47: **Kontrola shody architektury řešení projektu se vzory sdílených služeb eGovernmentu**				
Název architektonického vzoru eGovernmentu		**Byl dodržen vzor?**	**Č. žádosti o výjimku**	**Podrobný popis způsobu a míry dodržení vzorů návrhem řešení projektu**
Digitální služby a elektronické formuláře				
	Máte zajištěno předvyplňování elektronických formulářů všemi údaji subjektu, které veřejné správa zná?	Nerelevantní		Design digitálních služeb a elektronických formulářů není předmětem obsahu tohoto projektu, který zajišťuje řešení kybernetické bezpečnosti.
	Jsou veškeré služby poskytované klientům veřejné správy propojení s Katalogem služeb veřejné správy?	Nerelevantní		
Elektronický systém spisové služby				

Tabulka 47: **Kontrola shody architektury řešení projektu se vzory sdílených služeb eGovernmentu**				
Název architektonického vzoru eGovernmentu		**Byl dodržen vzor?**	**Č. žádosti o výjimku**	**Podrobný popis způsobu a míry dodržení vzorů návrhem řešení projektu**
	Je realizace propojení předmětu projektu se spisovou službou dle Národního standardu?	Nerelevantní		
Propojený datový fond				
	Využíváte pro překlad identity mezi agendami služby ISZR?	Nerelevantní		Propojený datový fond není v rámci projektu řešen, neboť projekt se zaměřuje na zvýšení kybernetické bezpečnosti lokálního perimetru žadatele.
	Je veškerá výměna údajů mezi ISVS realizována pomocí referenčního rozhraní (ISZR, eGSB/ISSS)?	Nerelevantní		
Elektronická identita				
	Využíváte služeb Národního bodu pro identifikaci a autentizaci?	Nerelevantní		Elektronická identita není v rámci projektu řešena. Projekt řeší lokální kybernetickou bezpečnost.
	Používáte pro překlad identifikátoru identity do své agendy (BSI na AIFO) služeb ISZR?	Nerelevantní		
	Využíváte při obsazení identifikované a autentizované osoby do role úředníka systém CAAIS (dříve JIP/KAAS)?	Nerelevantní		

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

3. DALŠÍ ÚDAJE O PROJEKTU

3.1. Majetkoprávní vztahy projektu

Tabulka 48: **Majetkoprávní vztahy**

Podmínka	Odpověď	Poznámka (důvod)
Budou vám udělena výhradní práva k užívání k dodávanému produktu?	Ne	Nebudeme pořizovat řešení na míru. Plánujeme nákup typového řešení, ke kterému nebudeme mít výhradní práva.
Budou vám udělena nevýhradní práva k užívání k dodávanému produktu?	Ano	Plánujeme nákup typového řešení ke kterému nebudeme mít výhradní práva.
Budou práva k autorskému dílu nějak omezena (IČO, konkrétní uživatel, převoditelnost a další šíření, úpravy produktu, parametry…)?	Ne	
Budete mít přístup ke zdrojovému kódu pro čtení?	Ano	V některých částech plánovaného řešení ano.
Bude vám či třetímu subjektu umožněno provádět údržbu, měnit produkt, upravovat jej či rozšiřovat bez souhlasu dodavatele?	Ne	
Budete mít přístup k aktuální technické dokumentaci produktu?	Ano	
Obsahuje budoucí smlouva ujednání o vyloučení odpovědnosti za výpadky fungování?	Ne	
Budou externí nákupy veřejně soutěženy?	Ano	Plánujeme soutěžit v souladu se zákonem o zadávání veřejných zakázek.
Bude celé nebo část řešení publikováno nebo bude využívat Open Source?	Ano	Kupříkladu dohled a monitoring je postaven na open-source Zabbix[6]. Nebo dále je užit Linux Debian[7].

3.2. Finanční připravenost projektu

Tabulka 49: **Finanční připravenost**

Druh financování	Odpověď	Popis zajištění, získání financování
Financování pomocí ESIF8	Ano	IROP 2021-2027, 10. výzva
Financování z vlastních zdrojů	Ano	Část bude financována z vlastních zdrojů (50 % CZV + NV) a část s využitím výzvy IROP (50 % CZV).
Financování pomocí jiných externích zdrojů	Ne	

3.3. Metodická připravenost projektu

Tabulka 50: **Metodická připravenost**

Metodické zajištění	Odpověď	Popis
Řízení pomocí metodiky (uveďte název)	Ano	Projektová metodika PRINCE2 s přihlédnutím k rozsahu projektu. Architekturní oblast je řízena pomocí metodiky TOGAF 10, architekturní prvky a vazby použité v konceptech jsou v souladu se specifikací **ArchiMate 3.2**. Bezpečnostní oblast je souladu se ZoKB/VKB, ISMS směrnicemi, metodikou SABSA a také doporučeními NÚKIB.

[6] Zabbix - Zabbix is an open-source software tool to monitor IT infrastructure such as networks, servers, virtual machines, and cloud services.
[7] Debian GNU/Linux - is a Linux distribution composed of free and open-source software and optionally non-free firmware or software.
[8] Evropské strukturální a investiční fondy

Tabulka 50: **Metodická připravenost**		
Metodické zajištění	**Odpověď**	**Popis**
Podpora od projektové kanceláře úřadu/resortu	Ano	Projektová kancelář existuje, kontakty kapitola 1.1
Podpora od architektonické kanceláře úřadu/resortu	Ano	Architekt je připraven k součinnosti a podpoře, kontakty kapitola 1.1
Bude tento formulář součástí zadávací dokumentace projektu?	Ano	

3.4. Personální náročnost projektu

Tabulka 51: **Vysvětlete personální náročnost projektu, jako odhady dopadu do počtu systemizovaných míst, či kapacitní náročnost realizace projektu dle FTE:**
V souvislosti s realizací projektu plánujeme navýšit personální obsazení o min. 2 FTE. Počítáme tak s dopadem na počet systemizovaných míst (rolí) a to v duchu specializovaných pozic, které jsou dány příslušnou platnou lokální legislativou a musí být obsazeny. • 82/2018 Sb. – **manažer KB** (§7, odst. 1), **architekt KB** (§7, odst. 2), **auditor KB** (§7, odst. 4) • 110/2019 Sb. – **pověřenec ochrany (zpracování) osobních údajů** (§14) Agendy, pravomoci a zodpovědnosti těchto rolí a základní rozsahy jejich kvalifikací jsou naznačeny v přílohách lokálních legislativních rámců nebo jako podpůrný materiál v rámci NÚKIB – bezpečnostní role. V rámci odkazovaného materiálu jsou pak popsány spádové oblasti organizačních a technických opatření vůči nimž jsou role důležité. Ultimativní výklad rolí, výstupů a agend bezpečnostních rolí možno čerpat na EU úrovni z materiálů ENISA[9] (ESCF[10]). Role věcných správců (garantů aktiv), technických správců a provozovatelů jsou uvedeny v **Tabulce 3** a také v business pohledu – Aplikační služby vs. Business Role. V rámci **Administrativní připravenost**i tohoto projektu je definován tým, který bude schopen pokrýt aktivity s projektem spojené. Přesná specifikace rolí a pravomocí/zodpovědností je popsána **v kapitole 4.5.3 ve Studii proveditelnosti projektu**, která je přílohou tohoto formuláře žádosti.

3.5. Harmonogram projektu

Tabulka 52: **Hrubý harmonogram předloženého projektu**				
Fáze / milník	**Začátek**	**Konec**	**Základní náplň**	**Navazuje na**
Přípravná fáze	01/2024	06/2024	Zpracování analýzy výchozího stavu ICT infrastruktury MČP10, formulace projektového záměru včetně technického řešení, zpracování žádosti o stanovisko Hlavního architekta eGovernmentu k plánovanému projektu zahrnujícímu záměr realizovat výdaj související s informačními a komunikačními technologiemi, zpracování průzkumu trhu, zpracování žádosti o poskytnutí dotace včetně veškerých relevantních příloh	
Zpracování zadávacích dokumentací a realizace veřejných zakázek	10/2024	06/2027	Zpracování zadávacích dokumentací (včetně technických specifikací, požadavků na implementaci, smluvních podmínek) a realizace nadlimitních veřejných zakázek	Přípravná fáze
Realizační fáze	4/2025	10/2027	Dodávka předmětu plnění veřejných zakázek (HW, SW vybavení) pro implementaci technických opatření, současně implementace organizačních opatření (viz studie proveditelnosti).	Realizace veřejných zakázek na předmět plnění
Provozní fáze	12/2027	12/2032	Zajištění kybernetické bezpečnosti.	Realizační fáze

[9] **ENISA** - The European Union Agency for Cybersecurity
[10] **ESCF –** European Cybersecurity Skills Framework

Tabulka 53: **Související projekty (v rozvojovém programu, portfoliu úřadu)**	
Předchozí projekty	**Popis návaznosti na předchozí projekty**
Bezpečné připojení 22 městských částí – Firewally pro MČ Praha 10 (MHMP)	Z projektu MHMP dodán 1 FW pro ochranu sítě Mepnet / KIVS, ale je tam i druhá VDOM použitelná pro potřeby MČ Praha 10. Na tento FW navazujeme dokupem dalšího FW do HA a dále dalších 2 FW do geograficky oddělené lokality.
Souběžné projekty	**Popis návaznosti na souběžné projekty**
Dodávka, implementace a podpora technologie DC Interconnect	Uživatel Mepnet / KIVS pro přístup do CMS. I v tomto předcházejícím projektu dochází k zajištění hospodárnosti a efektivitě projektů v rámci MČP10.
Ostatní projekty s MHMP	Koordinace a strategie transformace je zvažována dobře a kontinuálně, dochází k dynamické komunikaci mezi řízením projektů MHMP a MČP10.
Navazující projekty	**Popis návaznosti na budoucí projekty**
Celoměstské projekty MHMP	Participace na budoucích celoměstských projektech řešících zejména oblasti kybernetické bezpečnosti (FW, ISMS, SIEM/SOC, NOC, Backup/Restore, Antivir…), centrální nákup licencí apod.

Tabulka 54: **Vysvětlení dalších údajů o projektu**
Hlavním cílem projektu je zvýšení kybernetické bezpečnosti aktiv Úřadu MČ Praha 10, tedy jeho informačních systémů včetně informací v nich spravovaných. Tohoto cíle bude dosaženo realizací dílčích cílů zaměřených na řešení dále uvedených problémů. Dílčími cíli projektu jsou ve své podstatě naplněná opatření organizačního a technického rázu odpovídající zákonu 181/2014 Sb. v rozsahu specifikovaném detailněji vyhláškou 82/2018 Sb. Také je nutno začlenit problematiku zpracování osobních údajů v celé její šíři, což je rozsahem zákona 110/2019 Sb.

3.6. Zhodnocení ekonomické výhodnosti

3.6.1. Ekonomické parametry projektu

Hrubý odhad hodnoty záměru nákupu služeb či investic a provozních či rozvojových výdajů (externích výdajů)**, souvisejících s informačními a komunikačními technologiemi** (projektu).

.

Tabulka 55: Ekonomické parametry projektu			
Souhrnná položka dle metodiky TCO [Kč] bez DPH	**① Výdaje na realizaci (výstavbu) projektu**	**② Výdaje na provoz a rozvoj (do konce plánované smlouvy)**	**Vysvětlení k položce**
Počet měsíců trvání fáze	30	60	
A. Předběžné analýzy (vč. rizik), tvorba zadání, výběr řešení, výběr dodavatele – náklady nákupního procesu	1 784 628,-		Zpracování komplexní dotační žádosti včetně žádosti na OHA, příprava veřejných zakázek včetně technických specifikací, předimplementačních analýz, řízení projektu, dotační administrace a ostatní servisní práce.
B. Nákup SW a HW pro projekt (bez SaaS či PaaS)	54 066 116,-		Pořízení HW a SW nástrojů definovaných ve studii proveditelnosti.
C. Analýza, finální projekt, vývoj, implementace, školení uživatelů, zkušební provoz a testy, případně i migrace dat a akceptační audit	2 000 000,-		Implementace bezpečnostních organizačních opatření
D. Provoz a podpora řešení HW a SW (bez SaaS či PaaS)		33 340 000,-	Provozní náklady v pětiletém horizontu (výdaje spojené se zajištěním základní podpory provozu pořizovaného vybavení).
E. Hardware/Software údržba a průběžné úpravy (bez SaaS či PaaS)		0	
F. Projekty postupné inovace a zlepšování (plánované)	0	0	
G. Projekty upgrade (pokud jsou plánovány)	0	0	
H. Zvýšené náklady užívání řešení vč. nákladů na přechod z předchozího řešení (pokud se vyskytnou)	0	0	

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

Tabulka 55: Ekonomické parametry projektu			
Souhrnná položka dle metodiky TCO [Kč] bez DPH	**① Výdaje na realizaci (výstavbu) projektu**	**② Výdaje na provoz a rozvoj (do konce plánované smlouvy)**	**Vysvětlení k položce**
I. Útlum, konzervace a ukončení řešení	0	0	
X. Licence, HW, provoz, podpora, údržba, průběžný rozvoj – vše v subskripci (pouze SaaS a PaaS)	0	0	
Z. Ostatní nerozlišené režijní náklady	0	2 000 000,-	Ostatní provozní výdaje v pětiletém horizontu - osobní výdaje, výdaje na dopravu, telefon, počítač, kancelář atd. spojené se zajištěním administrativní kapacity v době udržitelnosti projektu.
Celkem	**57 850 744,-**	**35 340 000,-**	**Ceny bez DPH (ve studii proveditelnosti, kap. 11 uvedeny včetně DPH)**

3.6.2. Celkové náklady vlastnictví (TCO) funkčního celku

Ekonomická náročnost funkčního celku, který je tímto projektem měněn či vyvíjen, založený na Metodice výpočtu TCO ICT služeb veřejné správy.

Tabulka 56: **Nevyplnění tabulky**	
Následující tabulku 57 není třeba vyplňovat, pokud má žadatel vyplněny informace o funkčním celku v rejstříku informačních systémů veřejné správy.	Nevyplněno z důvodu existence údajů z RISVS

Tabulka 57: Celkové náklady vlastnictví (TCO) funkčního celku					
Souhrnná položka modelu TCO	① Interní náklady úřadu	② Náklady jiného úřadu VS	③ Náklady úřadu na externí služby	④ Náklady celkem	Vysvětlení k položce TCO
PLÁNOVÁNÍ A PŘÍPRAVA (včetně závěrečného návrhu realizace)					
A. Plánování, analýzy, zadání, výběr řešení a dodavatele				∑	
REALIZACE (projektu)					
B. Pořízení SW a HW pro projekt (ne v případě Cloud)				∑	
C. Vývoj, implementace/integr. a zkušební provoz				∑	
PRODUKČNÍ PROVOZ (včetně řízených změn)					
D. Provoz a podpora řešení (ne v případě Cloud)				∑	
E. Údržba, opravy a průběžné úpravy (ne v případě Cloud)				∑	
F. Projekty postupného zlepšování řešení (plánované)				∑	
G. Projekty upgrade (pokud jsou plánovány)				∑	
H. Zvýšené náklady užívání řešení (pokud se vyskytnou)				∑	Nepovinné, uveďte jen, je-li pro funkční celek významné
X. Řešení jako služba (pouze SaaS)				∑	
VYHODNOCENÍ					
Z. Ostatní, k fázi životního cyklu nepřiřaditelné režijní náklady				∑	Nepovinné, uveďte jen, je-li pro funkční celek významné
UKONČENÍ SLUŽBY (produkčního provozu)					
I. Útlum, konzervace a ukončení řešení					
Celkové TCO projektu (5let)	∑	∑	∑	∑	

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

Tabulka 58: **Vysvětlení a komentář ke zhodnocení ekonomické výhodnosti**

Ekonomická náročnost projektu je detailně popsána v přiložené Studii proveditelnosti. Pro celkový obraz očekávaných výdajů se prováděl průzkum trhu a trasovaly se ceny obvyklé. K stanovení rozsahů pak pro projekt posloužila studie proveditelnosti jako zdroj přesných informací v patřičných souvislostech.

Kód položky MS2021+	Položka rozpočtu v MS2021+	Položka rozpočtu	Celková cena za položku v Kč včetně DPH
1	**Celkové výdaje**		**69 999 400**
1.1	Celkové způsobilé výdaje (přímé + nepřímé)		**69 999 400**
1.1.1	Celkové způsobilé výdaje – přímé výdaje		**65 420 000**
1.1.1.1	Celkové způsobilé výdaje – investiční	4 x FC Switch	2 662 000
1.1.1.1	Celkové způsobilé výdaje – investiční	8 x LAN ToR Switch	3 388 000
1.1.1.1	Celkové způsobilé výdaje – investiční	2 x LAN management Switch	363 000
1.1.1.1	Celkové způsobilé výdaje – investiční	3 x NG Firewall	2 360 000
1.1.1.1	Celkové způsobilé výdaje – investiční	Webový aplikační FW	787 000
1.1.1.1	Celkové způsobilé výdaje – investiční	Nástroj pro VPN	787 000
1.1.1.1	Celkové způsobilé výdaje – investiční	Nástroj pro vícefaktorové ověřování	2 118 000
1.1.1.1	Celkové způsobilé výdaje – investiční	Nástroj pro detekci kybernetických bezpečnostních událostí	6 958 000
1.1.1.1	Celkové způsobilé výdaje – investiční	E-mail protection	1 785 000
1.1.1.1	Celkové způsobilé výdaje – investiční	Nástroj na sběr a vyhodnocování logů	2 148 000
1.1.1.1	Celkové způsobilé výdaje – investiční	SIEM	6 958 000
1.1.1.1	Celkové způsobilé výdaje – investiční	Technologický aplikační monitoring	2 118 000
1.1.1.1	Celkové způsobilé výdaje – investiční	DLP	2 239 000
1.1.1.1	Celkové způsobilé výdaje – investiční	Nástroj pro vulnerability skenování	1 301 000
1.1.1.1	Celkové způsobilé výdaje – investiční	Nástroj pro správu privilegovaných účtů	2 538 000
1.1.1.1	Celkové způsobilé výdaje – investiční	Nástroj na sběr a vyhodnocování logů z firewallů	1 198 000
1.1.1.1	Celkové způsobilé výdaje – investiční	Sandbox	2 166 000
1.1.1.1	Celkové způsobilé výdaje – investiční	10 x Server	3 751 000
1.1.1.1	Celkové způsobilé výdaje – investiční	10 x Server pro SDS	3 509 000
1.1.1.1	Celkové způsobilé výdaje – investiční	2 x Storage (SAN)	8 107 000
1.1.1.1	Celkové způsobilé výdaje – investiční	Zálohování	2 118 000
1.1.1.1	Celkové způsobilé výdaje – investiční	Endpoint security management	2 057 000
1.1.1.1	Celkové způsobilé výdaje – investiční	Ochrana a správa mobilních zařízení - MDM	1 072 000
1.1.1.1	Celkové způsobilé výdaje – investiční	EZS serverovna	569 000
1.1.1.1	Celkové způsobilé výdaje – investiční	Kamerový systém serverovna	400 000
1.1.1.1	Celkové způsobilé výdaje – investiční	Elektronický přístupový systém serverovna	426 000
1.1.1.1	Celkové způsobilé výdaje – investiční	Serverová UPS	1 174 000
1.1.1.2	Celkové způsobilé výdaje – neinvestiční	Penetrační testy	363 000
1.1.2	**Nepřímé náklady**		**4 579 400**
1.2	Celkové nezpůsobilé výdaje		**0**

Pozn.: ceny uvedeny včetně DPH v souladu s implementační metodikou IROP.

Tabulka 58: **Vysvětlení a komentář ke zhodnocení ekonomické výhodnosti**
Výše nepřímých výdajů se předpokládá 4 579 000,- Kč včetně DPH, které nemají vazbu na realizaci technických opatření dle zákona. Z těchto výdajů budou hrazeny náklady přípravné fáze (Předběžné analýzy (vč. rizik), tvorba zadání, výběr řešení, výběr dodavatele – náklady nákupního procesu) a náklady na implementaci bezpečnostních organizačních opatření.

4. VYJÁDŘENÍ K BEZPEČNOSTNÍM ASPEKTŮM

Tabulka 59: **Předkladatel prohlašuje, že předkládaný projekt bude realizován plně v souladu s níže uvedeným prohlášením**
Text vyplňujte až na případnou výzvu OHA.

5. UPOZORNĚNÍ A DOPORUČENÍ

Tabulka 60: **Upozornění a doporučení**

6. PŘÍLOHY

Tabulka 61: **Přílohy**		
Typ	**Číslo a název přílohy**	**Upřesnění přílohy**
Architektonický model	EA metamodel - Městská část Praha 10.xml	TOGAMEFF xml (výměnný standardní formát metamodelu v notaci ArchiMate 3.2)
Výstup z architektonického nástroje	EA metamodel - Městská část Praha 10.html	Referenční export do single page HTML z ArchiMateTool 5.3 (elementy, vazby, popisy)
Analýza	Studie proveditelnosti Kyberbezpečnost Praha 10.pdf	Studie proveditelnosti projektu
Jiný	o1_Zapis_RV_CMK_08-11-2023_.pdf	Zápis z komise celoměstských projektů
Jiný	o1_Zapis_RV_CMK_dd-mm-rrrr_.pdf	Zápis z komise celoměstských projektů
Celkový počet příloh:	5	