**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 MV**

****

**Praha, leden 2022**

**verze 7.1**

**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>

1. Základní informace o PROJEKTU
	1. Úvodní informace o žadateli o stanovisko k plánovanému projektu

| Tabulka 1: **Úvodní informace o žadateli o stanovisko** |
| --- |
| **Organizace žadatele** | Obec s rozšířenou působností | Masarykova 769 | 00036512 |
| **Ředitel pro informatiku nebo Statutární zástupce** | Jan Novák | ředitel odboru informatiky | jan.novak@orp.cz | 738 569 32 |
| **Kontaktní osoba projektu** | Petr Svoboda | projektový manažer | petr.svoboda@orp.cz | 725 334 698 |
| **Architekt projektu** | Jiří Dvořák | architekt | jiri.dvorak@orp.cz | 745 288 972 |
| **Verze předkládaných / doplněných žádostí o stanovisko, data jejich předložení a jejich čísla jednací** |
| **Číslo předkládané verze:** | **Datum předložení:** | **Verze předložena pod Čj,:** |
| **1.0** | **4. 2. 2022** |  |
|  |  |  |
|  |  |  |
|  |  |  |

| 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)** | ***Ne*** |
| **Výzvy v Integrovaném regionálním operačním programu** (IROP), **vypište číslo výzvy** | *Doplnit číslo výzvy IROP* |
| **Dobrovolná žádost o stanovisko** | ***Ne*** |

* 1. Shrnutí charakteristik projektu

| Tabulka 3: **Shrnutí charakteristik projektu** |
| --- |
| **Název projektu:** | Zajištění kybernetické bezpečnosti informačního systému obce s rozšířenou působností |
| **Specifický cíl / účel projektu:** | Hlavním cílem projektu je zvýšení kybernetické bezpečnosti informačního systému obce s rozšířenou působností za pomoci vhodných nástrojů tvořených softwarem, hardwarem a kvalitní bezpečnostní dokumentací.Předmětem projektu je také proškolení zaměstnanců pracujících v ORP a s tím související zvýšení jejich povědomí o kybernetické bezpečnosti. Výstupem projektu tak není pouze prostá dodávka zařízení pro detekci incidentů, ale i rovněž předcházet bezpečnostním incidentům v podobě preventivních opatření.  |
| **Seznam žádostí, které již byly v souvislosti s celkovými cíli a specifickým cílem / účelem projektu předány OHA:** | - |
| **Odkazy** [**na agendy VS**](https://rpp-ais.egon.gov.cz/gen/agendy-detail/)**, kterých se projekt týká:**  | Existuje agenda **A1721 Kybernetická bezpečnost**, avšak působnost zákona č. 181/2014 Sb. o kybernetické bezpečnosti, a tedy působnost této agendy se na obce s rozšířenou působností vztahuje jen za předpokladu, že jsou správci významného informačního systému případně systému kritické infrastruktury nebo základní služby. |
| **Seznam služeb veřejné správy a jejich úkonů z**[**katalogu služeb veřejné správy**](https://portal.gov.cz/sluzby-verejne-spravy/#/)**, kterých se projekt týká:** | Nerelevantní |
| **Odkazy na** [**určené IS**](https://rpp-ais.egon.gov.cz/AISP/verejne/isvs/zobrazeni-isvs) **dle UV 86/2020 a zákona 365/2000 Sb., kterých se projekt týká:** | *Přímo dotčené určené IS, které projekt realizuje nebo mění* | **Následující systémy jsou uvedeny pouze na ukázku. Každá obec s rozšířenou působností bude disponovat mnoha různými systémy, což zde nelze zachytit.**7666 – SYDO Traffic DSA (dopravně správní agenda)1163 – IS Ginis (spisová služba)1162 – MISYS (územní plánování, správa majetku apod.)1161 – Kvasar Ovzduší SQL  |
| *Nepřímo dotčené určené IS* | Viz poznámka k přímo dotčeným informačním systémům. |
| **Názvy a odkazy na** [**projekty v katalogu Digitálního Česka nebo jejich ID a názvy**](https://archi.gov.cz/znalostni_baze%3Aseznam_zameru_dc)*Nebo informace, proč není součástí katalogu Digitální Česko. Financování z tohoto programu nehraje roli, jedná se o jednotný katalog všech ICT záměrů veřejné správy.* | - |
| **Termíny:** |
|  | **Zahájení realizace projektu:** | **Spuštění první služby do produkčního prostředí:** | **Ukončení provozní smlouvy plánované v tomto projektu:** |
|  |  |  |  |
| **Výhrady ke zveřejnění formuláře:** |
|  | **Formulář obsahuje veřejné informace a předpokládáse jeho zveřejnění. Pokud se zveřejněním nesouhlasíte, uveďte důvod, případně úpravy, které budou nutné, aby bylo zveřejnění možné:**  | *Neveřejné jsou informace o tom, zda je žadatel povinnou osobou dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB); dále pak informace obsažené v tabulce č. 34: Dopady narušení bezpečnosti informací v systému. Tyto informace nebudou na základě výjimky dle § 10a ZKB veřejnosti poskytovány* |
| **Výjimky:** |
|  | **Žádáte výjimku/y vyplývající z nedodržení architektonických principů eGovernmentu nebo jiných skutečností?** | ***Ne*** | **Počet žádostí o výjimku/y v přílohách:** |  |
| **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* | **Manažer kybernetické bezpečnosti** |
| **Technický správce** *Subjekt, který zajišťuje technickou realizaci požadavků věcného správce k předmětu projektu* | **Obec s rozšířenou působností** |
| **Provozovatel** *Subjekt, který zajišťuje provoz HW a SW předmětu projektu* | **Obec s rozšířenou působností** |
| **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****<uveďte jako přílohu>* |
| **Realizační** (implementační) **výdaje v rámci projektu** (součet hodnot ve sloupci ① tabulky 51) **v Kč bez DPH:** | **Částka bude závislá na konkrétním projektu** |
| **Provozní výdaje plánované v rámci projektu** (součet hodnot ve sloupci ② tabulky 51) **v Kč bez DPH:** | **Částka bude závislá na konkrétním projektu** |
| **Pětileté TCO projektu** (součet hodnot ve sloupci ③ tabulky 51) **v Kč bez DPH:** | **Částka bude závislá na konkrétním projektu** |

* 1. Popis, potřebnost a výstupy projektu

| Tabulka 4: **Popis projektu** |
| --- |
| **Popis výchozí situace projektu** (tzv. As-Is, současný stav)**:** |
| Organizace a její procesy:Výchozí situaci obce s rozšířenou působností v oblasti kybernetické bezpečnosti lze hodnotit jako značně neuspokojivou. Obec nemá zpracovanou žádnou dokumentaci, která by se týkala kybernetická bezpečnosti. Všechny bezpečnostní incidenty se řeší nahodile a bez standardizovaného postupu. Obec dále nedisponuje vnitřními předpisy, které by upravovaly pravidla kybernetické bezpečnosti. Nedostatečné nastavení pravidel vede k rizikovému chování zaměstnanců obce s rozšířenou působností, a v tom důsledku ke zvýšené míře kybernetických bezpečnostních incidentů. Celá tato situace je rovněž umocněna tím, že zaměstnanci nejsou dostatečně proškoleni.Technické řešení:Obec s rozšířenou působností disponuje pouze základní technickou infrastrukturou k zajišťování kybernetické bezpečnosti. V provozu je kamerový systém, který má zamezit pohybu nepovolaných osob v budově. Hlídání budovy úřadu je zajišťováno bezpečnostní agenturou. V oblasti informačních systémů samosprávného celku neexistují žádná pravidla pro přihlašování a úřad nedisponuje softwarem ani technologií k zajištění sledování síťového provozu a monitoringu aplikací. Uživatelé se do různých systémů hlásí prostřednictvím různých hesel, která si musejí pamatovat, což není pohodlné. Vícefaktorová autentizace není v systémech využívána. Servery jsou zabezpečeny příslušným antivirovým softwarem a jsou uloženy ve vyhovujícím prostředí se zajištěním nepřerušeného napájení (UPS). Celý prostor je monitorován kamerami se záznamem v režimu 24/7. Přístup je dovolen pouze určitým osobám, což zajišťuje čtečka čipových karet.ORP dosud nedisponuje systémem, který by detekoval a vyhodnocoval bezpečnostní incidenty. K vyhodnocování incidentů nejsou přiřazeni žádní pracovníci. V současnosti neprobíhá ani sběr logů. Žadatel tudíž nemá žádný přehled o tom, co se děje v jeho informačním systému. Jakýkoliv bezpečnostní incident tak není včas zachycen a může celé organizaci způsobit značnou újmu, co do správného fungování informačního systému.  |
| **Popis cílové situace po dosažení celkového cíle / cílů projektu** (tzv. To-Be, budoucí stav)**:** |
| Hlavní cílem je zvýšení kybernetické bezpečnosti informačních systémů obce s rozšířenou působností. Tohoto cíle bude dosaženo realizací několika dílčích cílů zaměřených na řešení uvedených problémů. Dílčími cíli jsou:1) vypracování bezpečnostní dokumentace a její průběžná aktualizace,2) vypracování interních předpisů obsahujících pravidla kybernetické bezpečnosti a zajištění jejich dodržování,3) proškolení zaměstnanců v oblasti kybernetické bezpečnosti,4) pořízení softwarových nástrojů a technologií za účelem zajištění monitoringu,5) pořízení softwaru za účelem ochrany před škodlivým kódem (antivirový program).Cílová situace ohledně kybernetické bezpečnosti obce s rozšířenou působností by měla být taková, aby její zaměstnanci měli povědomí o bezpečnostních rizicích, vyvarovali se rizikového chování a dokázali pružně a efektivně reagovat na nastalé bezpečnostní incidenty. Do cílového stavu lze zahrnout i určité zajištění prevence před bezpečnostními incidenty, čehož bude dosaženo, jak výše uvedenými opatřeními, tak speciálními nástroji pro monitoring a analýzu síťového provozu. Vytvoření dokumentace a zavedení pravidel pak umožní v kombinaci se systémy pro detekci bezpečnostních incidentů včasnou reakci na tyto incidenty a jejich řešení.  |
| **Popis změn, tzn. výsledků / výstupů projektu nezbytných k dosažení jeho specifického cíle / účelu:** |
| Zásadní změnou bude vypracování bezpečnostní dokumentace a její udržování v aktuálním stavu. Vypracování dokumentace a její aktualizace bude zajištěna externím subjektem, neboť samosprávný celek nedisponuje dostatečnou znalostí problematiky kybernetické bezpečnosti. Bezpečnostní dokumentace bude obsahovat především pravidla pro uchovávání a vytváření hesel a vydefinované procesy, podle kterých bude nutné postupovat v případě bezpečnostního incidentu. Dalším krokem je zajištění dostatečných znalostí o kybernetické bezpečnosti u zaměstnanců samosprávného celku prostřednictvím zajišťování pravidelných školení k problematice kybernetické bezpečnosti. Dále bude pořízen potřebný software a hardware pro monitorování bezpečnostních rizik a zajištění prevence před možnými bezpečnostními incidenty. |
| **Důvody realizace projektu** (označte všechny relevantní)**:** |
| Legislativní důvody |[ ]  Konec licencí | ☐ |
| Modernizace, optimalizace řešení (výsledky business analýz) |[ ]  Lepší nabídka trhu |[ ]
| Požadavky zaměstnanců, uživatelů |[x]  Konec podpory od dodavatele |[ ]
| Konec podpory produktu, vynucené modernizace nižších vrstev |[ ]  Jiné (vysvětlete v tabulce 8) |[x]
| Hospodárnost |[ ]   |  |
| **Přehled zvažovaných alternativ řešení rozdílných od „Popisu projektu“** (tzv. To-Be) **specifikovaného výše:** |
| **Varianta 1 – Nulová varianta**Při nulové variantě nebude ORP kybernetickou bezpečnost vůbec dále rozvíjet. Nulová varianta povede k tomu, že ORP nebude dostatečně připraven na kybernetické hrozby. Pokud se ORP 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 náklady ještě výrazně vyšší. **Varianta 2 – Provozní varianta**Při zachování současného stavu nebude ORP dostatečně připravena 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 ORP vystavena velkému nebezpečí odcizení dat, případně poškození důležitých aplikací informačního systému. **Varianta 3 – Rozvojová varianta**Realizací projektu dojde k odstranění nejpalčivějších problémů kybernetické bezpečnosti ORP. 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 projektu bude značně sníženo riziko poškození informačních systému, případně odcizení dat.**Obec s rozšířenou působností preferuje třetí, tedy rozvojovou variantu.** |

| Tabulka 5: **Přehled výstupů projektu** |
| --- |
| **Označení výstupu** | **Množství a jednotka** | **Celková cena výstupu** [Kč] | **Plánovaná životnost výstupu [rok]** | **Vysvětlení výstupu** |
| Zpracování bezpečnostní dokumentace a její udržování | 1 ks |  |  | Kvalitní bezpečnostní dokumentace je nezbytným nástrojem k dosažení cíle tohoto projektu. Díky bezpečnostní dokumentaci budou jasně definovaná pravidla i procesy, jak bojovat s bezpečnostními incidenty, jakož i další pravidla, která zajistí prevenci před takovými incidenty. |
| Školení pro zaměstnance v oblasti kybernetické bezpečnosti | 1 ks |  |  | Bez proškolených zaměstnanců a jejich znalosti potenciálních kybernetických hrozeb nelze zajistit uplatňování bezpečnostních pravidel v praxi. |
| Log management | 1 ks |  |  | Pořízení komponenty log managementu umožní sledovat chování zaměstnanců ORP v informačním systému díky čemu bude možné předcházet rizikům s bezpečností. |
| Správa identit a řízení přístupů | 1 ks |  |  | Komponenta zajistí jednotné přihlašování k aplikacím, které se v rámci informačního systému ORP využívají (počítá se s principem Single Sign on). Uživatelé si již nebudou muset pamatovat přihlašovací údaje k jednotlivým aplikacím. Komponenta zahrnuje rovněž řízení přístupů k aplikacím a nastavení přístupových práv.  |
| SIEM | 1 ks |  |  | Jedná se o komponentu, která zajistí vyhodnocování případných bezpečnostních hrozeb. |
| Antivirový software | 1 ks |  |  | Antivirový software zajistí ochranu informačního systému před škodlivým kódem. |

* 1. 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?** | **Ne** |
| **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?** | **Ne**  |
| **Druh informačního / komunikačního systému dle klasifikace stanovené zákonem č. 181/2014 Sb., o kybernetické bezpečnosti** | **Významný informační systém**  |
| **Bezpečnostní úroveň informačního systému dle vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci** | **Bezpečnostní úroveň neurčena** |

* 1. 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 informačními systémy) je zvýšení jejich informovanosti o možných kybernetických rizicích, což jim v případě potřeby umožní vypořádat se s bezpečnostními incidenty a předcházet jim. Jasně definovanými pravidly bude zajištěno, že každý zaměstnanec bude v případě bezpečnostního incidentu vědět, jak se chovat a jak bezpečnostním incidentům předcházet. Při práci s informačními systémy budou mít zaměstnanci jistotu zabezpečení před odcizením citlivých dat a údajů. Nastavená pravidla umožní pružnou reakci na potencionální bezpečnostní incidenty tak, aby nebylo ohroženo poskytování služeb.Celkové přínosy pro uživatele výstupu projektu tak lze definovat následovně:1) rozšíření povědomí o kybernetických rizicích u zaměstnanců územního samosprávného celku,2) jasně definované postupy předcházení a řešení kybernetických bezpečnostních incidentů,3) zvýšení důvěry zaměstnanců v používané informační systémy,4) zlepšení ochrany dat a citlivých údajů o jejich subjektech. |
| **Přínosy na straně věcného správce** (zvýšení kvality jeho výstupů, snížení pracnosti na straně jeho úředníků aj.)**:** |
| Přínosem pro věcného správce je v první řadě zlepšení kvality poskytování služeb. Díky zvýšení kybernetické bezpečnosti bude značně omezeno riziko odcizení citlivých dat a údajů. Věcný správce bude mít jistotu, že služby budou poskytované prostřednictvím zabezpečených informačních systémů. Věcný správce dále získá nové nástroje (bezpečnostní dokumentace a proškolené zaměstnance), díky kterým bude moci předcházet bezpečnostním incidentům a efektivně je řešit v případě že nastanou.Celkové přínosy pro věcného správce projektu lze definovat následovně:1) poskytování bezpečných služeb, u kterých je významně sníženo riziko odcizení dat a údajů,2) dispozice jasně definovanými postupy a pravidly,3) dispozice zaměstnanci, kteří jsou znalí problematiky kybernetické bezpečnosti. |
| **Přínosy pro technického správce a provozovatele služby** (snížení energetické náročnosti, zjednodušení a úspora pracnosti správy systému, snížení výdajů na provoz aj.)**:** |
| Předcházení bezpečnostním incidentům a jejich efektivní řešení v první řadě přispěje k větší spolehlivosti provozovaného softwaru a infrastruktury.  |

| Tabulka 8: **Vysvětlení k základním podmínkám dosažení přínosů (nutným předpokladům a rizikům dosažení celkového cíle / cílů) projektu** |
| --- |
| Cíl projektu může být ohrožen spoustou různých rizik a naopak spousta okolností může přispět ke zdárnému dokončení projektu a dosažení definovaného cíle. Jednotlivé faktory jsou zachyceny v následující SWOT analýze.

|  |  |  |
| --- | --- | --- |
| **Interní faktory** | **Silné stránky:**Jasně definované a nastavené bezpečnostní procesy a pravidlaZaměstnanci se znalostí problematiky kybernetické bezpečnostiInfrastruktura a SW pro monitoring bezpečnostních incidentů | **Slabé stránky:**Na chování podle pravidel bude potřebné si navyknoutOmezené zdroje samosprávného celku (pracovníci, finance) |
| **Externí faktory** | **Příležitosti:** Výrazně menší riziko úniků dat a informacíSnížení nákladů na odstraňování následků bezpečnostních incidentů | **Hrozby:**Objeví se nové typy kybernetického nebezpečíZaměstnanci si nedokážou osvojit nová pravidla a procesyProcesy a pravidla nebudou řádně aktualizovány, aby dokázaly reagovat na nejnovější hrozbyPořízení nevhodných výstupů (dokumentace, nástroje, školení) během realizace projektu, které nezajistí dosažení definovaného cíle |

 |

1. Architektonické informace o projektu
	1. Dodržení architektonických principů NA VS ČR

| Tabulka 9: **Dodržení architektonických principů Národní architektury veřejné správy ČR** |
| --- |
| **Klasifikace** | **Vyberte** | **Č. žádosti o výjimku** | **Vysvětlete** |
| [Standardně digitalizované](https://archi.gov.cz/ikcr) | **Nerelevantní** |  | <Dodržení principu je dle mapující tabulky [NAP](https://archi.gov.cz/nap_dokument%3Auvod#zakladni_architektonicke_principy_a_jejich_naplneni)>  |
| [Zásada „pouze jednou“](https://archi.gov.cz/ikcr) | **Nerelevantní** |  | <Dodržení principu je dle mapující tabulky [NAP](https://archi.gov.cz/nap_dokument%3Auvod#zakladni_architektonicke_principy_a_jejich_naplneni)> |
| [Podpora začlenění a přístupnost](https://archi.gov.cz/ikcr) | **Nerelevantní** |  | <Dodržení principu je dle mapující tabulky [NAP](https://archi.gov.cz/nap_dokument%3Auvod#zakladni_architektonicke_principy_a_jejich_naplneni)> |
| [Otevřenost a transparentnost](https://archi.gov.cz/ikcr) | **Nerelevantní** |  | <Dodržení principu je dle mapující tabulky [NAP](https://archi.gov.cz/nap_dokument%3Auvod#zakladni_architektonicke_principy_a_jejich_naplneni)> |
| [Přeshraniční přístup jako standard](https://archi.gov.cz/ikcr) | **Nerelevantní** |  | <Dodržení principu je dle mapující tabulky [NAP](https://archi.gov.cz/nap_dokument%3Auvod#zakladni_architektonicke_principy_a_jejich_naplneni)> |
| [Interoperabilita jako standard](https://archi.gov.cz/ikcr) | **Nerelevantní** |  | <Dodržení principu je dle mapující tabulky [NAP](https://archi.gov.cz/nap_dokument%3Auvod#zakladni_architektonicke_principy_a_jejich_naplneni)> |
| [Důvěryhodnost a bezpečnost](https://archi.gov.cz/ikcr) | **Ano** |  | <Dodržení principu je dle mapující tabulky [NAP](https://archi.gov.cz/nap_dokument%3Auvod#zakladni_architektonicke_principy_a_jejich_naplneni)> |
| [Jeden stát](https://archi.gov.cz/ikcr) | **Nerelevantní** |  | <Dodržení principu je dle mapující tabulky [NAP](https://archi.gov.cz/nap_dokument%3Auvod#zakladni_architektonicke_principy_a_jejich_naplneni)> |
| [Sdílené služby veřejné správy](https://archi.gov.cz/ikcr) | **Nerelevantní** |  | <Dodržení principu je dle mapující tabulky [NAP](https://archi.gov.cz/nap_dokument%3Auvod#zakladni_architektonicke_principy_a_jejich_naplneni)> |
| [Připravenost na změny](https://archi.gov.cz/ikcr) | **Ano** |  | <Dodržení principu je dle mapující tabulky [NAP](https://archi.gov.cz/nap_dokument%3Auvod#zakladni_architektonicke_principy_a_jejich_naplneni)> |
| [eGovernment jako platforma](https://archi.gov.cz/ikcr) | **Nerelevantní** |  | <Dodržení principu je dle mapující tabulky [NAP](https://archi.gov.cz/nap_dokument%3Auvod#zakladni_architektonicke_principy_a_jejich_naplneni)> |
| [Vnitřně pouze digitální](https://archi.gov.cz/ikcr) | **Nerelevantní** |  | <Dodržení principu je dle mapující tabulky [NAP](https://archi.gov.cz/nap_dokument%3Auvod#zakladni_architektonicke_principy_a_jejich_naplneni)> |
| [Otevřená data jako standard](https://archi.gov.cz/ikcr) | **Nerelevantní** |  | <Dodržení principu je dle mapující tabulky [NAP](https://archi.gov.cz/nap_dokument%3Auvod#zakladni_architektonicke_principy_a_jejich_naplneni)> |
| [Technologická neutralita](https://archi.gov.cz/ikcr) | **Nerelevantní** |  | <Dodržení principu je dle mapující tabulky [NAP](https://archi.gov.cz/nap_dokument%3Auvod#zakladni_architektonicke_principy_a_jejich_naplneni)> |
| [Uživatelská přívětivost](https://archi.gov.cz/ikcr) | **Nerelevantní** |  | <Dodržení principu je dle mapující tabulky [NAP](https://archi.gov.cz/nap_dokument%3Auvod#zakladni_architektonicke_principy_a_jejich_naplneni)> |
| [Konsolidace a propojování](https://archi.gov.cz/ikcr)  | **Nerelevantní** |  | <Dodržení principu je dle mapující tabulky [NAP](https://archi.gov.cz/nap_dokument%3Auvod#zakladni_architektonicke_principy_a_jejich_naplneni)> |
| [Omezení budování monolitických systémů](https://archi.gov.cz/ikcr) | **Nerelevantní** |  | <Dodržení principu je dle mapující tabulky [NAP](https://archi.gov.cz/nap_dokument%3Auvod#zakladni_architektonicke_principy_a_jejich_naplneni)> |

* 1. 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**](http://www.opengroup.org/subjectareas/enterprise/archimate/model-exchange-file-format) | *Zvolte položku.* |
| **Případně vysvětlete, proč není model přiložen ve standardizovaném formátu či není přiložen vůbec.** |  |

* + 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)**:** |
| --- |
| Základním cílem, k jehož naplnění směřuje realizace projektu je zvýšení kybernetické bezpečnosti ORP. Důvodů pro zvýšení bezpečnosti je několik. ORP chce mít především k dispozici zpracovanou bezpečnostní dokumentaci, která vydefinuje, jak reagovat na bezpečnostní incident v případě, že nastane. Dále chce ORP zvýšit povědomí o kybernetických hrozbách u svých pracovníků, a to tím, že jim zajistí proškolení. Vyškolení zaměstnanci mnohem lépe rozpoznají bezpečnostní rizika a dokážou na ně adekvátně reagovat. Pro ORP je rovněž důležité snížení rizika odcizení citlivých dat a údajů, zajištění aby zaměstnanci pracovali s bezpečnými informačními systémy a aby byly prostřednictvím systémů poskytovány kvalitní a bezpečné služby. Jedním z výstupů je proto pořízení monitorovacího softwaru, který zajistí sledování nežádoucího chování a prevenci před bezpečnostními incidenty. Jelikož ORP zpravidla nebudou spadat mezi povinné subjekty podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti, 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“.Nakonec je nutné podotknout, že aktivity obce směřující ke zvýšení kybernetické bezpečnosti jsou omezeny zdroji, které má k dispozici. Jedná se především o finance a lidské zdroje.  |

| Tabulka 12: Katalog prvků motivační architektury |
| --- |
| ID | Typ prvku | Jméno prvku | Popis prvku |
| 1 | Zainteresovaný | Obec s rozšířenou působností | Obec s rozšířenou působností je hlavním zainteresovaným subjektem. Jeho zájmem je mít své informační systémy dostatečně zabezpečené před možnými hrozbami uvnitř i vně. ORP obsahuje i další zainteresované subjekty (Radu, občany apod.), kteří mají zájem na zvýšení kybernetické bezpečnosti. |
| 2 | Hnací prvek | Možnost adekvátní reakce na bezpečnostní incident | V současné době nejsou v organizaci nastaveny žádné postupy nebo procesy, které by zajistili adekvátní reakci na bezpečnostní incidenty. Potřeba adekvátní reakce na bezpečnostní incidenty je tak velmi palčivá. |
| 3  | Hnací prvek | Práce v zabezpečeném prostředí informačních systémů | Uživatelé informačních systémů musí mít důvěru v systém, se kterým pracují. Musí vědět, že systém je dostatečně zabezpečený proti virům a dalším kybernetickým hrozbám, a že v tom důsledku je značně sníženo riziko pádu systému nebo odcizení údajů.  |
| 4 | Hnací prvek | Poskytování kvalitních a bezpečných služeb | ORP má zájem na poskytování kvalitních a bezpečných služeb, kterým budou uživatelé důvěřovat, a u kterých bude dostatečně podchyceno riziko odcizení dat, případně napadení systému poskytujícího služby. |
| 5 | Hnací prvek | Snížení rizika odcizení citlivých údajů a informací | Citlivá data a údaje je třeba chránit před vyzrazením, neboť může dojít k újmě na právech dotčených subjektů.  |
| 6 | Cíl | Zvýšení kybernetické bezpečnosti informačních systémů samosprávného celku | Hlavní cíl, kvůli kterému je projektový záměr realizován.  |
| 7 | Princip | Minimální bezpečnostní standard (NÚKIB) | Obec s rozšířenou působností nebude zpravidla povinným subjektem podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti. Z toho důvodu byl Národním úřadem pro kybernetickou a informační bezpečnost vydán dokument, který alespoň rámcově vymezuje pravidla kybernetické bezpečnosti pro subjekty, které pod uvedený zákon nespadají. |
| 8 | Výstup | Vytvoření a průběžná aktualizace bezpečnostní dokumentace | Jedním z výstupů je vytvoření kvalitní bezpečnostní dokumentace, která vydefinuje potřebné procesy reakce v případě bezpečnostních incidentů. Samotné vytvoření takové dokumentace je však jen polovinou úspěchu. Dokumentaci bude nutné rovněž udržovat v aktualizovaném stavu, protože jen tak může být zajištěna reakce na nejnovější kybernetická nebezpečí. |
| 9 | Výstup | Pořízení softwaru a nástrojů pro monitoring incidentů | Pořízení softwaru pro monitoring je nezbytné pro předcházení bezpečnostním incidentům. |
| 10 | Výstup | Proškolení zaměstnanců v oblasti kybernetické bezpečnosti | Zaměstnance je třeba proškolit v oblasti kybernetické bezpečnosti a zajistit tak jejich povědomí o kybernetických hrozbách. Dalším důvodem je zajistit, aby se zaměstnanci zdrželi rizikového chování a dokázali včas bezpečnostní incident rozpoznat a adekvátně na něj reagovat. |
| 11 | Výstup | Audit kybernetické bezpečnosti | Jedním z předpokladů zajištění bezpečnosti je pravidelné a nezávislé zhodnocení stavu kybernetické bezpečnosti v organizaci.  |
| 12 | Omezení | Limitované zdroje obce s rozšířenou působností | Dosažení cíle (zvýšení kybernetické bezpečnosti ORP) je limitováno zdroji, které má ORP k dispozici. Jedná se především o finance a lidské zdroje.  |

**Diagram motivační architektury**



* + 1. Efektivita projektu – výkonnostní architektura

| Tabulka 13: Vysvětlete dopad projektu na hospodárnost, účelnost, účinnost, časovou a kvalifikační náročnost a na kvalitu služeb v organizaci (viz metodika TCO zveřejněná [zde](https://archi.gov.cz/znalostni_baze%3Atco)): |
| --- |
| 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 ORP je veřejným zadavatelem, bude nutné všechny komponenty nového řešení soutěžit v zadávacím řízení. ORP tedy očekává, že tím bude vybrána ta nejlepší nabídka, která zajistí náležité uspokojení potřeb při adekvátním vynaložení finančních prostředků.Realizací předmětu projektu bude výrazně zvýšena kvalita poskytovaných služeb, neboť zaměstnanci a uživatelé budou pracovat se zabezpečenými systémy, u nichž bude výrazně sníženo riziko odcizení citlivých data a útoku na systém. ORP si od realizace slibuje především zvýšení povědomí pracovníků o kybernetických hrozbách a jejich pružnou reakci v případě výskytu takové hrozby. Díky tomu ORP nebude muset vynakládat prostředky na externí subjekty, které mají dostatečné znalosti a dokáží na bezpečnostní incidenty reagovat. To povede k značnému snížení vynakládaných finančních prostředků z rozpočtu ORP. Zvýšení povědomí pracovníků o kybernetických rizicích a především kodifikace pravidel předcházení těmto rizikům v ORP povede ke zvýšení prevence bezpečnostních rizik a následně ke snížení nákladů vynakládaných na jejich odstraňování. ORP musí mít neustále na paměti, že ani nejdokonalejší nástroje pro detekci rizik neochrání, pokud selže lidský faktor.  |

| Tabulka 14: 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 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

| Tabulka 15: Popis povinných objektivně ověřitelných ukazatelů výkonnosti (příklad získání a výpočtu hodnot je uveden v metodice k tomuto formuláři; pokud nejsou zde uváděné objektivně ověřitelné ukazatele běžně dostupné, jako mohou být např. údaje o spokojenosti uživatelů nebo preferencích el. služby před neelektronickou, musí být jejich získání zahrnuto do projektu a zohledněno ve zdrojích nezbytných pro jeho realizaci a provoz) |
| --- |
| Název nově zřizované nebo měněné služby  | Předpokládaný počet transakcí za rok | Náklady na dokončenou transakci bez DPH? [Kč]  | Jaké % uživatelů je spokojeno s poskytovanou službou? | Jaké % transakcí je úspěšně dokončeno?  | Jaké % uživatelů zvolí raději elektronickou formu služby než ne-elektronickou? |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

| Tabulka 16: Popis volitelných objektivně ověřitelných ukazatelů výkonnosti |
| --- |
| Název ukazatele | Předmět měření | Jednotka  | Očekávaná hodnota od | Očekávaná hodnota do  |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. Byznys architektura

| Tabulka 17: Katalog prvků byznys architektury |
| --- |
| ID | Typ prvku | Jméno prvku | Popis prvku |
| 1 | Aktér | Auditor kybernetické bezpečnosti | Jedná se o osobu, která provádí audit kybernetické bezpečnosti. Na tuto činnost je speciálně vyškolena. |
| 2 | Aktér  | Výbor pro řízení kybernetické bezpečnosti | Výbor je kolektivní orgán, který je v organizaci pověřen řízením a rozvojem kybernetické bezpečnosti. Zpravidla je tvořen manažerem kybernetické bezpečnosti a zástupcem vrcholového vedení organizace. |
| 3 | Aktér | Manažer kybernetické bezpečnosti | Hlavní osoba zodpovědná za nastavení systému bezpečnosti informací. |
| 4 | Aktér | Zástupce vrcholového vedení ORP | Osoba, která je součástí výboru pro řízení kybernetické bezpečnosti. Zastupuje zájmy ORP. |
| 5 | Aktér | Garant aktiva | Fyzická osoba pověřená organizací k zajištění rozvoje, použití a bezpečnosti aktiva.  |
| 6 | Aktér | Architekt kybernetické bezpečnosti | Architekt kybernetické bezpečnosti je zásadním aktérem, který navrhuje opatření kybernetické bezpečnosti a zajišťuje jejich implementaci. |
| 7 | Byznys funkce | Řízení a rozvoj kybernetické bezpečnosti | Hlavní funkce v organizaci týkající se kybernetické bezpečnosti. Zajišťuje rozvoj a řízení všech aspektů, které se kybernetické bezpečnosti týkají. |
| 8 | Byznys proces | Audit kybernetické bezpečnosti | Proces, který má za cíl nezávisle zhodnotit stav kybernetické bezpečnosti organizace.  |
| 9 | Byznys proces | Zhodnocení úrovně kybernetické bezpečnosti | Ověřuje úroveň kybernetické bezpečnosti organizace a schopnost organizace reagovat na bezpečností rizika.  |
| 10 | Byznys proces | Posouzení souladu s dokumentací, právními předpisy a nejlepší praxí | Ověřuje shodu skutečného stavu v organizaci se stavem, který vyžadují právní předpisy a nejlepší praxe v oblasti kybernetické bezpečnosti.  |
| 11 | Byznys funkce | Systém řízení bezpečnosti informací | Tento systém je tvořen zavedením a udržováním jednotlivých opatření kybernetické bezpečnosti. |
| 12 | Byznys funkce | Určení chráněných aktiv | Určení významných aktiv, která je nutná chránit před bezpečnostními incidenty. |
| 13 | Byznys funkce | Stanovení rizik bezpečnosti | Určení okolností, která představují rizika pro organizaci a její bezpečnost.  |
| 14 | Byznys funkce | Zavedení opatření bezpečnosti | Zavedení opatření, která organizaci ochrání před kybernetickými riziky. |
| 15 | Byznys proces | Řízení rizik bezpečnosti | Proces zaměřený na správu rizik bezpečnosti, jejich aktualizaci, doplnění a případně vypuštění.  |
| 16 | Byznys proces | Kontrola opatření | Kontrola opatření nastavených v organizaci a jejich dodržování. |
| 17  | Byznys proces | Zajištění rozvoje, použití a bezpečnosti aktiva | Klasifikace aktiv z pohledu bezpečnosti jejich použití a nastavení pravidel pro jejich rozvoj. |
| 18 | Byznys proces | Návrh bezpečnostních opatření | Návrh opatření s cílem eliminovat či zmírnit dopad bezpečnostních incidentů na organizaci a její systémy.  |
| 19 | Byznys proces | Implementace bezpečnostních opatření | Implementace opatření s cílem zvýšit kybernetickou bezpečnost organizace. |
| 20 | Byznys proces | Řízení dodavatelů | Proces řízení dodavatelů má předejít nejčastějším problémům, jakými jsou vendor lock, nedostatečná ochrana poskytnutých informací a nedostatečná opatření při správě systémů. |
| 21 | Byznys proces | Řízení změn | Proces zajišťuje správu a vyhodnocování změn, které mohou mít vliv na kybernetickou bezpečnost organizace. |
| 22 | Byznys proces | Řízení lidských zdrojů | Proces zajišťuje zvyšování povědomí o kybernetických rizicích u zaměstnanců organizace, zejména prostřednictvím jejich školení. |
| 23 | Byznys proces  | Řízení kontinuity činností | Cílem procesu je zajištění obnovy funkčnosti organizace v případě výskytu mimořádné události. |
| 24 | Byznys produkt | Business continuity plan | Plán obnovy. |
| 25 | Byznys produkt | Disaster recovery plan | Havarijní plán. |
| 26 | Byznys produkt | Legislativa | Legislativa ovlivňující činnosti v oblasti kybernetické bezpečnosti. Jedná se především o zákon č. 181/2014 Sb. o kybernetické bezpečnosti a vyhlášku č. 82/2018 Sb. o kybernetické bezpečnosti. |
| 27 | Aktér | Uživatel aktiv | Osoba využívající aktiva ORP. |
| 28 | Aktér | Povinná osoba | Jedná se o osobu, která je odpovědná za detekci kybernetických bezpečnostních incidentů, jejich vyhodnocení a zpracování. |
| 29 | Událost | Detekce kybernetického bezpečnostního incidentu | Detekce kybernetických bezpečnostních incidentů, které se v organizaci vyskytnou.  |
| 30 | Byznys proces | Hodnocení a hlášení kybernetických bezpečnostních incidentů | Náplní procesu je správné vyhodnocování kybernetických bezpečnostních incidentů, jejich koordinace a nahlášení příslušným orgánům. |

| 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 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:** |  |
|  | Portál poskytující služby klientům využívá design dle <https://designsystem.gov.cz/>  | 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 doe-Podatelny** | **Nerelevantní** |  |
| **Listinnou cestou do podatelny** | **Nerelevantní** |  |

| 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 v NIA) a druh autentizace** | **Vysvětlete autorizaci ve službě (přidělení role, mandáty, zastupování, atd.)** |
| Systém identity managementu | Jedná se o interní nástroj sloužící k identifikaci uživatelů pracujících se systémy ORP | Uživatelské jméno a heslo | Jednotlivé role přiděluje pověřený administrátor |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Model byznys architektury (výkonu veřejné správy) – pohled činnostních funkcí**



**Model byznys architektury (výkonu veřejné správy) – pohled služeb veřejné správy**

****

| Tabulka 20: **Vysvětlení kontextu byznys architektury úřadu** |
| --- |
| 1. **jaké k projektu existují či vznikají duplicity a proč?**
 |
| V projektu neexistují ani nevznikají duplicity. |
| 1. **jsou využity všechny sdílené služby?**
 |
|  |
| **Vysvětlení byznys architektury projektu:** |
| Primárním cílem je zvýšení kybernetické bezpečnosti organizace a snížení dopadů kybernetických rizik. Nejdůležitější aktérem je v tomto ohledu výbor kybernetické bezpečnosti skládající se z manažera a zástupce vedení ORP (např. člen rady ORP popřípadě tajemník). Výbor bude mít odpovědnost za řízení a rozvoj kybernetické bezpečnosti v organizaci. Manažer kybernetické bezpečnosti je zodpovědný za nastavení systému řízení bezpečnosti informací, především za určení aktiv a jejich zranitelnosti, nastavení 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. Auditor je osoba s příslušnou odborností a posuzuje soulad opatření nastavených v organizaci s právními předpisy a s nejlepší praxí v oblasti kybernetické bezpečnosti. Za návrh bezpečnostních opatření a jejich implementaci je odpovědný architekt kybernetické bezpečnosti. Za zajištění rozvoje, použití a bezpečnosti aktiva je zodpovědný příslušný garant. Pohled služeb veřejné správy zachycuje proces detekce, vyhodnocování a hlášení kybernetických bezpečnostních incidentů.  |

* + 1. Architektura informačních systémů (aplikací a dat)
			1. Architektura informačních systémů – část: Aplikační architektura

| Tabulka 21: Katalog všech aplikačních komponent řešení a klíčových aplikačních funkcí |
| --- |
| ID | Typ prvku | Jméno prvku | Popis prvku |
| **1** | Aplikační rozhraní | Webové rozhraní | Webové rozhraní sestává z portálových řešení, která umožňují přístup k jednotlivým systémům a práci s nimi. Rozhraní dále využívá standardní technologii SSL (Secured socket layer) k zabezpečení komunikace mezi uživatelem a systémem. |
| **2** | Aplikační komponenta | Informační systém ORP | Pohled na informační systém ORP. Jedná se pouze o typový systém, který se bude u každého ORP lišit v závislosti na jeho velikosti, množství užívaných aplikací a podobně.  |
| **3** | Aplikační komponenta | IS Ginis (spisová služba) | Aplikace zajišťuje výkon spisové služby.  |
| **4** | Aplikační komponenta | SYDO Traffic (dopravně-správní agenda) | Aplikace zajišťuje výkon dopravně-správní agendy.  |
| **5** | Aplikační komponenta | MISYS (Územní plánování a správa majetku) | Aplikace zajišťuje výkon agendy územního plánování a správy majetku ORP. |
| **6** | Aplikační komponenta | Log management | Komponenta je klíčová pro zaznamenávání chování uživatelů v jednotlivých systémech. Tím komponenta napomáhá k prevenci před bezpečnostními riziky a jejich detekci. |
| **7** | Aplikační komponenta | Správa identit a přístupů | Komponenta zajišťuje správu identit a přístupů k jednotlivým systémům ORP. |
| **8** | Aplikační komponenta  | SIEM | Komponenta SIEM (Security Information and Event Management) vyhodnocuje data a varuje před možnými bezpečnostními riziky. |
| **9** | Datový objekt | Záznam logů | Data zaznamenaná prostřednictvím komponenty Log managementu. Obsahuje data o chování uživatelů v systémech. |
| **10** | Datový objekt | Kmen identitních dat | Obsahuje data týkajících se identit a přístupových práv jednotlivých uživatelů, kteří pracují se systémy ORP. |
| **11** | Datový objekt | Bezpečnostní hrozby | Hrozby detekované komponentou SIEM. |
| **12** | Aplikační služba | Spisová služba | Jedná se o služby poskytované aplikací spisové služby IS Ginis. |
| **13** | Aplikační služba | Služby dopravně-správní agendy | Služby aplikace pro dopravně-správní agendu. |
| **14** | Aplikační služba | Služby správy majetku a územního plánování | Služby aplikace pro správu majetku a územního plánování. |
| **15** | Aplikační služba | Služby log managementu | Služby aplikace pro zachycení chování uživatelů v systémech ORP. |
| **16** | Aplikační služba | Služby správy identit a přístupů | Služby zajišťují správu identit uživatelů v ORP a jejich přístup k jednotlivým aplikacím. |
| **17** | Aplikační služba | Služby SIEM | Klíčové služby pro zajištění kybernetické bezpečnosti. Služby zajišťují analýzu a vyhodnocování hrozeb. |
| **18** | Aplikační funkce | Výkon spisové služby | Zachycuje funkcionality spisové služby IS Ginis např. založení spisů jejich správu a vyřízení a podobně. |
| **19** | Aplikační funkce | Výkon dopravně-správní agendy | Pohled na funkcionality aplikace pro zajišťování dopravně-správní agendy. |
| **20** | Aplikační funkce | Výkon územního plánování a správy majetku | Pohled na funkcionality aplikace pro zajišťování územního plánování a správy majetku. |
| **21** | Aplikační funkce | Funkce log managementu | Pohled na funkcionality komponenty, která zachycuje chování uživatelů v systémech ORP. |
| **22** | Aplikační funkce | Funkce správy identit a přístupů | Pohled na funkcionality komponenty pro správu identit a přístupů. |
| **23** | Aplikační funkce | Funkce komponenty SIEM | Zachycuje funkcionalitu komponenty SIEM. |

**Diagram aplikační architektury – pohled struktury aplikací**

****

**Diagram aplikační architektury – pohled komunikace aplikací**



| Tabulka 22: **Vysvětlení v kontextu aplikační architektury úřadu** |
| --- |
| 1. **jaké k projektu existují či vznikají duplicity?**
 |
| V projektu neexistují ani nevznikají duplicity. |
| 1. **proč a jsou využity všechny sdílené služby?**
 |
|  |
| **Vysvětlení aplikační architektury projektu:** |
| Pohled na strukturu aplikací zachycuje především informační systém ORP, který je tvořen celou řadou dalších komponent. Architektura však není schopna zachytit všechny aplikace, kterými mohou jednotlivé ORP disponovat. Proto je vybrán modelový příklad typického ORP, který zachycuje nejčastěji používané aplikace. Tyto aplikace pak slouží výhradně k výkonu agend ORP (ať už v samostatné nebo přenesené působnosti), které směřují především vně ke klientům veřejné správy. Z pohledu ORP 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. Pohled komunikace aplikací pak zachycuje především funkcionalitu jednotlivých komponent informačního systému a služby, které jsou poskytovány vně na základě výkonu agendy obce, klientům veřejné správy. Služby, které se však podílejí na zajištění kybernetické bezpečnosti ORP směřují hlavně dovnitř. Funkce a služby podílející se na zajištění kybernetické bezpečnosti jsou barevně odlišeny. Aplikační architektura tak názorně ukazuje, že pro ORP není důležité jen zajišťování služeb směřujících vně, ale rovněž ochrana bezpečnosti vlastního informačního systému proti kybernetickým hrozbám. |

* + - 1. Architektura informačních systémů – část: Datová architektura

| Tabulka 23: **Katalog objektů a subjektů:** |
| --- |
| **Objekt nebo subjekt, který je předmětem evidence** | **Vysvětlení objektu nebo subjektu** | **Označení objektu nebo subjektu dle** [**Agend VS**](https://rpp-ais.egon.gov.cz/gen/agendy-detail/) | **Je objekt čerpán nebo poskytován jiným subjektům?** |
| Log | Jedná se o data, která zachycují přístup a chování uživatelů v aplikacích ORP. |  | Není poskytován ani čerpán |
| Identita uživatelů a přístupová práva | Identity uživatelů aplikací ORP a přístupová práva. Zajišťuje přístup pracovníků ORP k aplikacím a práci v nich. |  | Není poskytován ani čerpán |
| Bezpečnostní hrozba | Hrozba představující riziko pro informační systém ORP. |  | Není poskytován ani čerpán |

| Tabulka 24: Využití datového fondu základních registrů a dalších agend |
| --- |
| Název | Použito | Vysvětlení |
| Základní registry |
| Způsob vedení datového kmene | 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:** |  |
|  | **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 |  |

| Tabulka 25: 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 jako takový neřeší přístup datům v informačních systémech ORP. Přístup k datům z komponent, které se podílejí na zajišťování kybernetické bezpečnosti, je však zajištěn, a to za účelem detekce hrozeb. |
| **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 26: **Nakládání s osobními a citlivými údaji**  |
| --- |
| **Způsoby identifikace subjektů (FO, PO) v informačním systému**  | AIFO | Ne | *Projekt neřeší identifikaci subjektů, je zaměřen na kybernetickou bezpečnost. Nerelevantní.* |
| IČO | Ne | *Nerelevantní.* |
| Rodné číslo | Ne | *Nerelevantní.* |
| Vlastní klientský identifikátor | Ne | *Nerelevantní.* |
| Jiný identifikátor | Ne | *Nerelevantní.* |
| **Předpokládaný počet subjektů údajů dotčených zpracováním osobních údajů v systému (orientační počet osob, jejichž údaje budou v systému zpracovávány)** | * Má-li OVM informační systém, kde jsou zpracovávány údaje více než 50 000 osob, je skoro jisté, že půjde o VIS.
* Má-li organizace informační systém, kde jsou zpracovávány údaje více než 125 000 osob, mohlo by jít o KII, pokud bude naplněno některé z odvětvových kritérií v příloze č. 1 řešeného nařízení.
* Má-li OVM informační systém, kde jsou zpracovávány údaje více než 300 000 osob, půjde vždy o KII.
* Specificky u provozovatelů základních služeb v oblasti zdravotnictví je pak jedno z dopadových kritérií „*kompromitace citlivých osobních údajů o více než 200000 osobách*“.
 |
| **Způsoby zavedení základních principů práce s osobními a citlivými údaji dle GDPR a zákona o zpracování osobních údajů** |
| **Zabezpečení zpracování:** | <vysvětlete využití: pseudonymizace, šifrování, integrity, důvěryhodnosti apod. dle článku 32 GDPR> |
| **Logování přístupů k osobním a citlivým údajům:** | <vysvětlete zajištění logování přístupů k osobním a citlivým údajům včetně následného prokazování v rámci bezpečnostních auditů> |
| **Používáte nakládání s osobními údaji na základě doloženého souhlasu subjektu údajů:**  | <vypište seznam a důvod> |
| **Ostatní:** | <případně vysvětlete další připravenost na práva dle GDPR nebo jejich neaplikovatelnost pro tento projekt> |

| Tabulka 27: **Vysvětlení v kontextu datové architektury úřadu** |
| --- |
| 1. **jaké k projektu existují či vznikají duplicity?**
 |
| K projektu neexistují ani nevznikají duplicity. |
| 1. **jsou využity všechny sdílené služby?**
 |
|  |
| **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). 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. |

* + 1. Technologická architektura – vrstva IT technologie (HW a SW)

| Tabulka 28: Katalog uzlů a klíčových funkcí nebo služeb |
| --- |
| ID | Typ prvku | Jméno prvku | Popis prvku |
| **1** | Seskupení | Primární lokalita | Primární lokalita pro běh systémů ORP. |
| **2** | Seskupení | Sekundární lokalita | Sekundární lokalita pro běh systémů ORP. |
| **3** | Zařízení | Firewall PL | Firewall primární lokality. |
| **4** | Zařízení | Firewall SL | Firewall sekundární lokality. |
| **5** | Systémový software | Sondy monitoringu PL | Sondy monitoringu primární lokality. |
| **6** | Systémový software | Zálohovací a archivační SW PL | Zálohovací a archivační software primární lokality.  |

**Diagram technologické architektury – pohled struktury IT technologické architektury**

| Tabulka 29: **Vysvětlení v kontextu technologické architektury úřadu** |
| --- |
| 1. **jaké k funkčnímu celku existují či vznikají duplicity?**
 |
| K projektu neexistují ani nevznikají duplicity. |
| 1. **jsou využity všechny sdílené služby?**
 |
|  |
| **Vysvětlení technologické architektury projektu:** |
| Technologická architektura je reprezentována prostředky, na kterých jsou provozovány aplikace ORP. Jde především o 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). |

* + 1. Technologická architektura – vrstva komunikační infrastruktury

| Tabulka 30: Katalog infrastrukturních komunikačních funkcí, sítí, cest a klíčových služeb |
| --- |
| ID | Typ prvku | Jméno prvku | Popis prvku |
| **1** | Komunikační síť | Síť úřadu | Síť ORP. |
| **2** | Komunikační síť | Lokální síť úřadu | Lokální síť ORP. |
| **3** | Komunikační síť | SAN síť úřadu | Síť sloužící pro připojení externích zařízení k serverům. |
| **4** | Technologická služba | Služby sítě | Služby poskytované sítí úřadu. |

**Diagram technologické architektury – pohled struktury komunikační infrastruktury**

| Tabulka 31: Využití sdílených služeb komunikační infrastruktury |
| --- |
| Název | Popis | Použito | Č. žádosti o výjimku |
| CMS | Pro publikaci služeb tohoto projektu je využito Centrální místo služeb – aplikace jsou publikovány prostřednictvím CMS  | Nerelevantní |  |
| KIVS | Využití komunikační infrastruktury veřejné správy, tj. fyzického propojení infrastruktury úřadů připojení k CMS | Ano |  |
| NDC | Umístění technologií do Národních datových center v perimetru CMS | Ne |  |
| Housing (IaaS) | Využití umístění vlastní HW infrastruktury do prostor datového centra třetí strany | Ne |  |

| Tabulka 32: **Vysvětlení v kontextu architektury komunikační infrastruktury úřadu** |
| --- |
| 1. **jaké k projektu existují či vznikají duplicity a proč?**
 |
| K projektu nevznikají ani neexistují duplicity. |
| 1. **jsou využity všechny sdílené služby?**
 |
|  |
| **Vysvětlení architektury komunikační infrastruktury projektu:** |
| Komunikační vrstva zajišťuje tok dat mezi jednotlivými aplikacemi ORP a dále zajišťuje komunikaci s vnějším světem. Tyto úkoly komunikační vrstvy jsou zajišťovány prostřednictvím sítí poskytujících síťové služby. |

* + 1. Bezpečnostní architektura

| Tabulka 33: Katalog bezpečnostní architektury projektu |
| --- |
| Dotčený nebo bezpečnostní prvek | Hrozba / riziko  | Vysvětlení způsobu zmírnění hrozby / rizika prvkem architektury včetně technických a organizačních opatření |
| Informační systém ORP | Rizikové chování uživatelů (pracovníků ORP) – ztráta hesla, práce s aplikacemi bez příslušných oprávnění | Ke zmírnění tohoto rizika bude implementována komponenta správy identit a přístupů. Počítá se se zavedením principu Single Sign on, což povede ke snížení rizika ztráty nebo zapomenutí přihlašovacích údajů. Řízení přístupů zajistí, že s aplikací bude pracovat oprávněná osoba a to pouze v mezích svých oprávnění. Tato hrozba bude rovněž zmírněna implementací komponenty log managementu. |
| Informační systém ORP | Bezpečnostní incident | Riziko výskytu bezpečnostních incidentů bude sníženo jednak samotnými zaměstnanci ORP, kteří díky implementaci řízení lidských zdrojů a školení získají větší povědomí o kybernetických hrozbách a o tom, jak se v případě incidentu chovat. Riziko bude dále sníženo implementací komponenty SIEM, která ve spolupráci s Log management zajistí vyhodnocování hrozeb.  |
| Informační systém ORP (komponenta identity management) | Odcizení údajů spravovaných komponentou identity managementu | Dojde-li k odcizení údajů z komponenty identity managementu, pak hrozí zneužití těchto údajů a v nejhorším případě i poškození informačního systému ORP nepovolaným uživatelem. Jako prevence před tímto rizikem bude zajištěno logování veškerých úkonů v informačním systému ORP a jejich důsledné vyhodnocování s využitím SIEM. Uživatelé budou také proškoleni a poučeni o využívání systému identity managementu.  |
| Informační systém ORP | Poškození systému a jeho nefunkčnost v důsledku bezpečnostního incidentu | I přes veškerou prevenci je nutné počítat s možností, kdy se systém v důsledku bezpečnostního incidentu stane nefunkčním. Pro tento případ budou připraveny kvalitní plány (business continuity plan a disaster recovery plan) za účelem zajištění plynulosti při výkonu činností ORP. |

|  |
| --- |
| Tabulka 34: **Dopady narušení bezpečnosti informací v systému** |
| **Možné dopady v případě narušení dostupnosti**  | V případě narušení dostupnosti je ohrožen výkon řady agend, které ORP vykonává. Jedná se například o agendu A117 – občanské průkazy, A1046 – agendu řidičů a další agendy. Narušením dostupnosti by tak bylo ohroženo nabírání žádostí a vydávání občanských a řidičských průkazů. Výčet agend, které by byly narušeny, se může lišit i v závislosti na tom, jak je řešen informační systém konkrétní ORP. |
| **Možné dopady v případě narušení důvěrnosti**  | Narušení důvěrnosti a ohrožení dat informačních systémů ORP se bude lišit v závislosti na tom, jak velký datový kmen konkrétní ORP zpracovává. Některá ORP 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 orgánům ORP. U ORP je možné se bavit o ohrožení dat v řádu tisíců až desetitisíců subjektů. |
| **Možné dopady v případě narušení integrity**  | Narušení integrity informací může zapříčinit práci s nesprávnými informacemi a poškodit práva oprávněných subjektů. Riziko narušení integrity ORP podstatně sníží pořízením komponenty log managementu a SIEM pro zaznamenávání nestandardního chování a vyhodnocování rizik. |
| **Je v rámci Vaší organizace určen jakýkoliv prvek kritické infrastruktury?** | *Zvolte položku.* |
| **Případně specifikujte ty určené prvky KI, jejichž činnost významně nebo zcela ovlivňuje tento posuzovaný informační systém:** | Záleží na konkrétním ORP. |

|  |
| --- |
| Tabulka 35: **Bezpečnostní opatření a zohlednění principu „security by design“** |
| **Bezpečnostní opatření dle** [**Minimálního bezpečnostního standardu NÚKIB**](https://www.nukib.cz/download/publikace/podpurne_materialy/2020-07-17_Minimalni-bezpecnostni-standard_v1.0.pdf) (dále jen „**MBS**“) | **Odpověď** | **Popis realizace, případně odůvodnění nezavedení** |
| **Organizační opatření** |
| Plán zavádění bezpečnostních opatření (kapitola 2.1 MBS) | Ano | ORP s vytvořením takového plánu počítá. |
| Klasifikace a ochrana informací (kapitola 3 MBS) | Ano | Zajištěno. Definováno v rámci byznys architektury. |
| Řízení dodavatelů (kapitola 4 MBS) | Ano | Zajištěno. Definováno v rámci byznys architektury. |
| Řízení lidských zdrojů (kapitola 5 MBS) | Ano | Zajištěno. Definováno v rámci byznys architektury. |
| Řízení změn (kapitola 6 MBS) | Ano | Zajištěno. Definováno v rámci byznys architektury. |
| Řízení kontinuity činností (kapitola 7 MBS) | Ano | Zajištěno. Definováno v rámci byznys architektury. |
| Audit kybernetické bezpečnosti (kapitola 8 MBS) | Ano | Zajištěno. Definováno v rámci byznys architektury. |
| Další opatření | Ano | Počítá se s pravidelným školením pracovníků ORP za účelem zvýšení jejich povědomí o kybernetických hrozbách a rizicích. Dále se počítá s pořízením komponent (Log management a SIEM) pro vyhodnocování bezpečnostních rizik. |
| **Technická opatření** |
| Fyzická bezpečnost (kapitola 9 MBS) | Ano | Zajištěno. ORP disponuje kamerovým systémem za účelem monitorování prostorů úřadu a místností se servery. Prostor úřadu je hlídán bezpečnostní agenturou. |
| Řízení přístupů(kapitola 10 MBS) | Ano | Přístup do místností se servery a infrastrukturou je chráněn čtečkou čipových karet. Vstup je povolen pouze oprávněným držitelům.  |
| Ochrana před škodlivým kódem (kapitola 11 MBS) | Ano | Zajištěno. Aplikace a infrastruktura jsou chráněny kvalitním antivirovým softwarem.  |
| Řešení kyberbezpečnostních událostí a incidentů (kapitola 12 MBS) | Ano | Zajištěno. Definování procesu pro řešení kyberbezpečnostních událostí a incidentů je jedním z výstupů projektu. Definováno na byznys vrstvě.  |
| 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.  |
| Kryptografické prostředky (kapitola 14 MBS) | Ano | Počítá se s využitím kryptografických prostředků.  |
| Zajišťování úrovně dostupnosti informací (kapitola 15 MBS) | Ano | Zajištěno v návaznosti na Business continuity plan.  |
| Požadavky v oblasti cloudových služeb (kapitola 16 MBS) | Není známo | Záleží na konkrétním řešení.  |
| 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.  |
| Ochrana webových aplikací (kapitola 17.2 MBS) | Ano | Zajištěno. Komunikace s aplikacemi pomocí kanálu zabezpečeného s využitím technologie SSL.  |
| Zabezpečení komunikace s externími systémy (kapitola 17.4 MBS) | Ano | Zajištěno. S externími systémy bude komunikováno výhradně s využitím zabezpečené komunikační infrastruktury.  |
| Další opatření | Ano | Mezi další opatření, která budou předmětem projektu zavedena, patří pravidelná školení zaměstnanců ORP za účelem získání povědomí o kybernetických hrozbách. Dále ORP počítá s nastavením bezpečnostních pravidel, procesů a s jejich důsledným uplatňováním v praxi.  |

| Tabulka 36: **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, pokud nejsou řádně nastavena pravidla pro detekci a hlášení bezpečnostních incidentů a také pravidla, která je nutná dodržovat pracovníky ORP za účelem předcházení bezpečnostním incidentům. 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 měl ORP vždy přihlížet.  |

* + 1. Shoda s pravidly, standardizace a dlouhodobá udržitelnost

| Tabulka 37: **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](https://www.mvcr.cz/clanek/centralni-nakup-produktu-cisco-systems.aspx) | Ne | Důvod nevyužití uveden v záhlaví. |
| [Centrální nákup produktů IBM](https://www.mvcr.cz/clanek/centralni-nakup-produktu-ibm.aspx) | Ne | Důvod nevyužití uveden v záhlaví. |
| [Centrální nákup produktů Microsoft](https://www.mvcr.cz/clanek/centralni-nakup-produktu-microsoft.aspx) | Ne | Důvod nevyužití uveden v záhlaví. |
| [Centrální nákup produktů Oracle](https://www.mvcr.cz/clanek/centralni-nakup-produktu-oracle.aspx) | Ne | Důvod nevyužití uveden v záhlaví. |
| [Centrální nákup produktů VMware](https://www.mvcr.cz/clanek/centralni-nakup-produktu-vmware.aspx) | Ne | Důvod nevyužití uveden v záhlaví. |
| [Centrální nákup CITRIX](https://www.mvcr.cz/clanek/centralni-nakup-produktu-citrix.aspx) | Ne | Důvod nevyužití uveden v záhlaví. |
| [Centrální nákup ICT komodit](https://www.mvcr.cz/clanek/centralni-nakup-ict-komodit.aspx) | Ne | Důvod nevyužití uveden v záhlaví. |
| [Centrální soutěžení KIVS](https://www.mvcr.cz/clanek/komunikacni-infrastruktura-verejne-spravy-a-centralni-misto-sluzeb-584441.aspx?q=Y2hudW09Mw%3d%3d) | Ne | Důvod nevyužití uveden v záhlaví. |

| Tabulka 38: Cloud Computing |
| --- |
| Požadavek | Odpověď | Vysvětlení |
| Bude pro řešení využito služeb cloud computingu dle výsledku ekonomické výhodnosti provozu? | Ano | Záleží na konkrétním žadateli, zda bude chtít využít služeb cloud computingu a samozřejmě na ekonomickém vyhodnocení provozu v cloudu.  |
| Uveďte odkaz na poptávku, nabídku nebo využívání z katalogu cloud computingu |  |

| Tabulka 39: Shoda se strategickými dokumenty |
| --- |
| Požadavek | Odpověď | Číslo žádosti o výjimku | Vysvětlení |
| Je řešení v souladu s Informační koncepcí úřadu? | Ano |  | Zde odkaz na informační koncepci konkrétního ORP. |
| Je řešení v souladu s Informační koncepcí ČR a cíli či principy Digitálního Česka? | Ano |  | Předmětem projektu je naplňován obecný architektonický princip Důvěryhodnost a bezpečnost. |
| Je řešení v souladu s NAP? | Nerelevantní |  | Předmět projektu se týká zvýšení kybernetické bezpečnosti ORP. Národní architektonický plán cílí především na řádné využívání centrálních sdílených služeb, což však není předmětem tohoto projektu. Proto nerelevantní. |

| Tabulka 40: **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 smlouvy o provozu a podpoře.  | Součást smlouvy o provozu a podpoře |

| Tabulka 41: **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 42: **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 byznys architektury.  |

* 1. Kontrola shody architektury řešení projektu s požadavky Národního architektonického plánu

| Tabulka 43: **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** |
| **Centrální místo služeb** |
|  | Publikujete aplikační služby řešené tímto projektem do CMS druhé generace? | Nerelevantní |  | Předmětem projektu je zvýšení kybernetické bezpečnosti. Neexistují aplikační služby, které bychom chtěli publikovat prostřednictvím CMS. |
| Přistupujete ke službám jiných ISVS prostřednictvím CMS druhé generace? | Nerelevantní |  |  |
| Jakým způsobem přistupujete do CMS druhé generace? | KIVS |  |  |
| Využíváte vlastní připojení do veřejného internetu? | Nerelevantní |  |  |
| **Univerzální kontaktní místo** |
|  | Publikujete na CzechPOINT všechny své samoobslužné služby tak, aby mohly být přístupné i asistovaně?  | Nerelevantní |  | Projekt řeší kybernetickou bezpečnost, nikoliv poskytování služeb klientům.  |
| Jste na centrálu CzechPOINT připojeni skrze systém CMS? | Nerelevantní |  |  |
| **Rozšířený backoffice úředníka** |
|  | Máte služby CzechPOINT@office integrovány do svých systémů? | Nerelevantní |  | Projekt řeší kybernetickou bezpečnost.  |
| Budou všechny interní aplikace dostupné z intranetu úřadu/resortu? | Nerelevantní |  |  |
| Bude využito principu Single Sign-On? | Ano |  | Plánováno za účelem zvýšení bezpečnosti a předcházení možným incidentům.  |
| **ÚEP včetně eFakturace** |
|  | Máte zajištěno předvyplňování formulářů ÚEP všemi státu známými údaji subjektu? | Nerelevantní |  | Projekt řeší kybernetickou bezpečnost. Nezabývá se poskytováním služeb klientům. |
| Máte zajištěn příjem a zpracování elektronických faktur? | Nerelevantní |  |  |
| **Elektronický systém spisové služby** |
|  | Je realizace propojení systému se spisovou službou vytvořena dle rozhraní definovaného v kapitole 9 Národního standardu? | Nerelevantní |  | Projekt řeší kybernetickou bezpečnost, proto nerelevantní.  |
| **Informační systém datových schránek** |
|  | Je prováděno automatické vytěžování přijatých formulářů do informačního systému? | Nerelevantní |  | Projekt řeší kybernetickou bezpečnost. Neřešíme v rámci tohoto projektu.  |
| Jakým způsobem je předmět projektu napojen na ISDS? | Nerelevantní |  |  |
| **Propojený datový fond** |
|  | Jste ke službám PPDF připojeni skrze CMS? | Nerelevantní |  | Propojený datový fond není v rámci projektu řešen, neboť projekt se zaměřuje na zvýšení kybernetické bezpečnosti. |
| Využíváte pro překlad identity mezi agendami služby ISZR? | Nerelevantní |  |  |
| Využíváte pouze údaje, které máte explicitně uvedeny v daném zákoně? | Nerelevantní |  |  |
| Odebíráte na údaje PPDF notifikace skrze služby ISZR? | Nerelevantní |  |  |
| 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 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 JIP/KAAS? | Nerelevantní |  |  |

1. Další údaje o projektu
	1. Majetkoprávní vztahy projektu

| Tabulka 44: 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 však 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  |  |
| 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? | Ne | Řešení je specifické. Nelze využít Open Source. |

* 1. Finanční připravenost projektu

| Tabulka 45: Finanční připravenost |
| --- |
| Druh financování | Odpověď | Popis zajištění, získání financování |
| Financování pomocí ESIF[[1]](#footnote-2) | Ano | IROP |
| Financování z vlastních zdrojů | **Ano** | Část bude financována z vlastních zdrojů a část s využitím výzvy IROP. |
| Financování pomocí jiných externích zdrojů | Ano | Část bude financována z vlastních zdrojů a část s využitím výzvy IROP. |

* 1. Metodická připravenost projektu

| Tabulka 46: Metodická připravenost |
| --- |
| Metodické zajištění | Odpověď | Popis  |
| Řízení pomocí metodiky (uveďte název) | Ano | Projektová metodika PRINCE2 s přihlédnutím k rozsahu projektu. |
| Podpora od projektové kanceláře úřadu/resortu | *Zvolte položku.* | Záleží na konkrétním ORP, zda bude mít k dispozici projektovou kancelář. |
| Podpora od architektonické kanceláře úřadu/resortu | *Zvolte položku.* | Záleží na konkrétním ORP, zda bude mít zřízenu architektonickou kancelář, případně architekta k dispozici. |
| Bude tento formulář součástí zadávací dokumentace projektu? | *Zvolte položku.* | Rozhodnutí závisí na konkrétním ORP. |

* 1. Personální náročnost projektu

| Tabulka 47: **Vysvětlete personální náročnost projektu, jako odhady dopadu do počtu systemizovaných míst, či kapacitní náročnost realizace projektu dle FTE:** |
| --- |
| V souvislosti s realizací projektu neplánujeme navýšit personální obsazení. Realizace projektu nebude mít dopad na počet pracovních míst.  |

* 1. Harmonogram projektu

| Tabulka 48: Hrubý harmonogram předloženého projektu |
| --- |
| Fáze / milník | Začátek | Konec | Základní náplň | Navazuje na |
| Závisí na konkrétním žadateli |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

| Tabulka 49: Související projekty (v rozvojovém programu, portfoliu úřadu) |
| --- |
| Předchozí projekty | **Popis návaznosti na předchozí projekty** |
|  |  |
|  |  |
| Souběžné projekty | **Popis návaznosti na souběžné projekty** |
|  |  |
|  |  |
| Navazující projekty | **Popis návaznosti na budoucí projekty** |
|  |  |
|  |  |

| Tabulka 50: **Vysvětlení dalších údajů o projektu** |
| --- |
| Účelem realizace projektu je zvýšení kybernetické bezpečnosti ORP a nastavení všech relevantních procesů a pravidel souvisejících. Projekt bude řízen standardizovanou projektovou metodikou, modifikovanou s přihlédnutím k jeho velikosti.  |

* 1. Ekonomické parametry projektu

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

**Plán předpokládané ekonomické náročnosti projektu založené na metodologii pětiletých celkových nákladů vlastnictví** (tzv. Total Costs of Ownership) **- účelové členění nákladů projektu.**

| Tabulka 51: TCO |
| --- |
| Souhrnná položka modelu TCO [Kč] bez DPH | ① Výdaje na realizaci (výstavbu) projektu | ② Výdaje na provoz a rozvoj (do konce aktuální smlouvy) | ③ TCO 5= ① + (②, přepočtené na 5 let) | Vysvětlení k položce |
| Počet měsíců trvání fáze | 0 | 0 | 0 |  |
| A. Předběžné analýzy (vč. rizik), tvorba zadání, výběr řešení, výběr dodavatele – náklady nákupního procesu  | 0 | 0 | 0 |  |
| B. Nákup SW a HW pro projekt(bez SaaS či PaaS) | 0 |  | 0 | <uveďte do tabulky 53 nebo samostatné přílohy rozpad výdajů, pokud výdaj přesahuje 10% celkové ceny projektu a současně přesahuje 1 mil. Kč> |
| C. Analýza, finální projekt, vývoj, implementace, školení uživatelů, zkušební provoz a testy, případně i migrace dat a akceptační audit  | 0 |  | 0 | <při jakékoliv částce uveďte do tabulky 53 nebo samostatné přílohy seznam rolí s počtem člověkodnů a cenu za člověkoden> |
| D. Provoz a podpora řešení HW a SW (bez SaaS či PaaS) |  | 0 | 0 | <uveďte do tabulky 53 nebo samostatné přílohy rozpad výdajů, pokud roční provoz a podpora přesahuje 20% celkové ceny řešení> |
| E. Hardware/Software údržba a průběžné úpravy (bez SaaS či PaaS) |  | 0 | 0 | <uveďte do tabulky 53 či samostatné přílohy rozpad výdajů, pokud roční údržba a průběžné úpravy přesahuje 20% celkové ceny řešení> |
| F. Projekty postupné inovace a zlepšování (plánované) | 0 | 0 | 0 |  |
| G. Projekty upgrade (pokud jsou plánovány) | 0 | 0 | 0 |  |
| H. Zvýšené náklady užívání řešení vč. nákladů na přechod z předchozího řešení (pokud se vyskytnou) | 0 | 0 | 0 |  |
| I. Útlum, konzervace a ukončení řešení | 0 | 0 | 0 | <uveďte do tabulky 53 nebo samostatné přílohy rozpad výdajů, pokud útlum, konzervace a ukončení řešení přesahuje 10% celkové ceny řešení> |
| X. Licence, HW, provoz, podpora, údržba, průběžný rozvoj – vše v subskripci (pouze SaaS a PaaS) | 0 | 0 | 0 | <uveďte do tabulky 53 nebo samostatné přílohy rozpad výdajů, pokud výdaj na SaaS a PaaS přesahuje 1 mil. Kč> |
| Z. Ostatní nerozlišené režijní náklady  | 0 | 0 | 0 | <uveďte do tabulky 53 nebo samostatné přílohy rozpad výdajů, pokud výdaj na nerozlišenou režii přesahuje 0,5 mil. Kč> |
| Celkem | 0 | **0** | **0** |  |

| Tabulka 52: **Popis funkčního celku, který je projektem rozšiřován či upravován (pokud existuje)** |
| --- |
| Projekt rozšiřuje architekturu úřadu o aspekt kybernetické bezpečnosti, na který doposud nebyl kladen příliš velký důraz. Popis rozšíření a úprav lze nalézt především na úrovni jednotlivých architektur (viz výše ve formuláři).  |
| **Plánované 5leté externí výdaje celého funkčního** celku (mimo tento projekt) [tis. Kč]**:** |  |

| Tabulka 53: **Vysvětlení a komentář k souhrnu výdajů a ekonomické náročnosti projektu** |
| --- |
| Zde záleží na konkrétním ORP. Z vysvětlení by mělo vyplývat, proč jsou výdaje vynakládány a proč zrovna ve stanovené výši (resp. jejich odůvodnění). |

1. Vyjádření k bezpečnostním aspektům

| Tabulka 54: **Předkladatel prohlašuje, že předkládaný projekt bude realizován plně v souladu s níže uvedeným prohlášením** |
| --- |
| *Text vyplňujte až na případnou výzvu OHA.* |

1. Upozornění a doporučení

| Tabulka 55: **Upozornění a doporučení** |
| --- |
|  |

1. Přílohy

| Tabulka 56: **Přílohy** |
| --- |
| **Typ** | **Číslo a název přílohy** | **Upřesnění přílohy** |
| *Zvolte položku.* |  |  |
| *Zvolte položku.* |  |  |
| *Zvolte položku.* |  |  |
| *Zvolte položku.* |  |  |
| *Zvolte položku.* |  |  |
| Celkový počet příloh: |  |

1. Evropské strukturální a investiční fondy [↑](#footnote-ref-2)