Zámer národného projektu[1]

Názov národného projektu (ďalej aj „NP“):
Kybernetická bezpečnosť v samospráve do 6 000 obyvateľov

Žiadateľ[2]:

Obchodné meno/názov	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
Právna forma	Rozpočtová organizácia
Sídlo	Pribinova 25
IČO	50349287

Poskytovateľ: Ministerstvo investícií, regionálneho rozvoja a informatizácie SR

Partner, ktorý sa bude zúčastňovať na implementácii aktivít NP (ak je to relevantné)

Obchodné meno/názov	
Právna forma	
Sídlo	
IČO	
Zdôvodnenie potreby partnera NP[3]	
Kritériá pre výber partnera[4]	
Má partner jedinečné postavenie na implementáciu týchto aktivít? Ak áno, na akom základe?	

V prípade viacerých partnerov, doplňte údaje za každého partnera.

Sumárne informácie o NP

Celkové oprávnené výdavky NP (v EUR)	13 433 863 Eur
Miesto realizácie projektu (na úrovni kraja, resp. celé územie Slovenskej republiky)	Celé územie Slovenskej republiky
Identifikácia hlavných cieľových skupín (ak relevantné)	
Projekt so špecifickým určením pre marginalizované rómske komunity[5]	nie

[1] Formulár zámeru NP predstavuje minimálny obsahový štandard, ktorý je poskytovateľ oprávnený dopĺňať a rozširovať na základe svojich potrieb.

[2] Uviesť aj názov sekcie, ak je to relevantné. Žiadateľom je osoba, ktorá žiada o poskytnutie príspevku do nadobudnutia účinnosti zmluvy o poskytnutí nenávratného finančného príspevku alebo právoplatnosti rozhodnutia podľa § 13 ods. 2 zákona č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, alebo osoba, ktorá predkladá zámer NP.

[3] Pod partnerom sa rozumie partner ako je definovaný v § 3, písm. t) zákona č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[4] Uveďte, na základe akých kritérií bol partner vybraný, alebo ak boli kritériá zverejnené, uveďte odkaz na internetovú stránku, kde sú dostupné. Ako kritérium pre výber partnera môže byť tiež uvedená predchádzajúca spolupráca žiadateľa s partnerom, ktorá bude náležite opísaná a odôvodnená, avšak nejde o spoluprácu, ktorá by v prípade verejných prostriedkov spadala pod pôsobnosť zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[5] Zo zoznamu sa vyberie:

- "**áno**" – ak, projekt bude financovaný výhradne z alokácie so špecifickým určením pre marginalizované rómske komunity (ďalej len „MRK“) uvedenej v Programe Slovensko,
- "**nie**" - ak, projekt nebude v žiadnej miere financovaný z alokácie so špecifickým určením pre MRK uvedenej v Programe Slovensko,
- "**čiastočne**" – ak, projekt bude z časti financovaný z alokácie so špecifickým určením pre MRK uvedenej v Programe Slovensko.

Spolufinancovaný Európskou úniou

Začlenenie národného projektu v štruktúre Programu Slovensko[6]

Cieľ politiky súdržnosti[7]	1 Konkurencieschopnejšia a inteligentnejšia Európa vďaka presadzovaniu inovatívnej a inteligentnej transformácie hospodárstva a regionálnej prepojenosti IKT
Priorita	1P1 Veda, výskum a inovácie
Špecifický cieľ	RSO1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy
Opatrenie (ak relevantné)	1.2.1 Podpora v oblasti informatizácie a digitálnej transformácie Vyberte položku. Vyberte položku.
Súvisiace typy akcií[8]	Zlepšovanie technologického, procesného, infraštruktúrneho, vedomostného a organizačného zabezpečenia zručností a kapacít pre plnenie úloh v oblasti KIB v prostredí orgánov štátnej a verejnej správy

Zákonné požiadavky

§ 23 ods. 3 zákona č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

1. Dôvod určenia prijímateľa NP[9]

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej ako „MIRRI SR“) je ústredným orgánom štátnej správy pre centrálne riadenie informatizácie spoločnosti a tvorbu politiky jednotného digitálneho trhu, rozhodovanie o využívaní verejných prostriedkov vo verejnej správe pre informačné technológie, centrálnu architektúru integrovaného informačného systému verejnej správy a koordináciu plnenia úloh v oblasti informatizácie spoločnosti (ust. § 10 ods. 1 písm. d) zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov).

MIRRI SR zabezpečuje úlohy národného prevádzkovateľa centrálnej informačnej infraštruktúry a centrálnej komunikačnej infraštruktúry Slovenskej republiky pre verejnú správu (ust. § 4 písm. a) zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe (ďalej len ako „ZoITVS“) a o zmene a doplnení niektorých zákonov) a zároveň je orgánom vedenia ITVS.

Na základe zákona o ITVS bola vydaná vyhláška č. 179/2020 Z. z. Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy. V zmysle uvedenej vyhlášky je potrebné, v rámci minimálnych bezpečnostných opatrení pre oblasť kybernetickej bezpečnosti vo verejnej správe, okrem iného, „ustanoviť plán rozvoja bezpečnostného povedomia, ktorý obsahuje

[6] V prípade zámeru NP, ktorý sa plánuje financovať z viacerých cieľov politiky súdržnosti / priorít / špecifických cieľov / opatrení sa vyberú zo zoznamu viaceré položky.
Zákon č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, Rámec implementácie fondov a metodický dokument č. 2 riadiaceho orgánu pre Program Slovensko neobmedzujú, resp. nevylučujú možnosť spojiť dva schválené zámery národných projektov do jednej výzvy, resp. na jeden schválený zámer národného projektu vyhlásiť dve výzvy na predloženie národných projektov. V takýchto prípadoch bude riadiaci orgán posudzovať výzvu tak, aby boli splnené všetky parametre schváleného/schválených zámeru/zámerov národného projektu berúc na zreteľ povolené odchýlky.

[7] V prípade Fondu na spravodlivú transformáciu sa vyberie "-".

[8] V súlade s informačným monitorovacím systémom.

[9] V prípade, ak ide o prijímateľa, ktorý nie je určený v Programe Slovensko, alebo ktorého kompetencie nevyplývajú z osobitných predpisov podľa zákona č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, príslušná komisia pri Monitorovacom výbore pre Program Slovensko schválením zámeru NP schvaľuje aj prijímateľa NP. V opačnom prípade sa prijímateľ NP neposudzuje.

formu, obsah a rozsah potrebných školení a vykonať bezpečnostné vzdelávanie na zvýšenie bezpečnostného povedomia najmenej každé tri roky.“

MIRRI SR je zároveň ústredným orgánom štátnej správy pre oblasť kybernetickej bezpečnosti v sektore verejná správa, podsektor informačné systémy verejnej správy podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov ((ďalej len ako „ZoKB“).MIRRI SR ako ústredný orgán pre podsektor informačné systémy verejnej správy buduje bezpečnostné povedomie, koordinovanú spoluprácu na všetkých stupňoch riadenia kybernetickej bezpečnosti a aplikuje bezpečnostné opatrenia a politiku správania sa v kybernetickom priestore (§ 9, ods. d) zákona o kybernetickej bezpečnosti).

MIRRI SR prevádzkuje, zákonom zriadenú, vládnu jednotku CSIRT (CSIRT.SK), ktorá poskytuje služby pre informačné systémy verejnej správy podľa zákona o kybernetickej bezpečnosti.
MIRRI SR je regulátorom a celoslovensky pôsobiacim orgánom pre oblasť bezpečnosti a riešenia kybernetických incidentov vo vzťahu k informačným systémom verejnej správy.

MIRRI SR poskytuje metodickú podporu povinným subjektom a zabezpečuje zvyšovanie spôsobilostí, vzdelávanie, skvalitnenie a rozvoj kybernetickej a informačnej bezpečnosti v sektore verejnej správy.

2. Odôvodnenie využitia NP

V zmysle zákona č.69/2018 Z.z. o kybernetickej bezpečnosti, je každá obec prevádzkovateľom základnej služby štátu a je povinná dodržiavať bezpečnostné opatrenia podľa §20 (1). Sú to úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov. Z tohto dôvodu MIRRI SR realizuje tento národný projekt, ako centralizovaný model riešenia, kde pre obce poskytne zvýšenie bezpečnostného štandardu oblasti kybernetickej a informačnej bezpečnosti (ďalej ako „KIB“) pre obce do 6000 obyvateľov v podobe procesného, technického, hardvérového vybavenia, aplikácií, SW ako aj zastrešenie zdieľanej funkcie IT security experta pre kybernetickú bezpečnosť. Na Slovensku sa nachádza 2 795 obcí s počtom obyvateľov do 6 000.

Centrálne koordinovaná dodávka v rámci projektu poskytuje unifikovaný a profesionálne garantovaný rámec pre všetky vecné oblasti. Výhodou je okrem iného aj zdieľanie zdrojov, jednotný bezpečnostný štandard, jednoduchšia kontrola, lepšie zmapovanie incidentov a kontinuálna metodická aj technická podpora. Realizácia prostredníctvom národného projektu je nielen efektívnejšia, ale aj udržateľnejšia z dlhodobého hľadiska a významne prispieva k zvýšeniu kybernetickej odolnosti celého segmentu verejnej správy.

3. Zdôvodnenie vylúčenia „súťažného postupu“ výberu projektu prostredníctvom výzvy

V správe o kybernetickej bezpečnosti v Slovenskej republike v roku 2023, Národného bezpečnostného úradu, sa uvádza, že najvyšší počet nahlásených kybernetických bezpečnostných incidentov v roku 2023 pochádzalo zo sektorov verejná správa, bankovníctvo a zdravotníctvo.

Cieľom projektu je zvýšenie kybernetickej a informačnej bezpečnosti v obciach do 6 000 obyvateľov. Projekt je vhodnejšie realizovať ako národný projekt, keďže obce často nedisponujú nie len dostatočnými finančnými zdrojmi, ale ani odbornými kapacitami, čo vyvoláva potrebu zamestnania externých odborníkov na kybernetickú bezpečnosť. Tým pádom obce nemusia cez výzvu žiadať o finančný prostriedok. Technológie a služby bude MIRRI SR objednávať až vtedy, keď jednotlivé obce predložia konkrétne požiadavky. Tento prístup zabezpečí, že nákup bude realizovaný podľa aktuálnej potreby, čím sa optimalizuje a účelovo nasmeruje čerpanie finančných prostriedkov, bude zabezpečená hospodárnosť a efektívnosť.

Spolufinancovaný Európskou úniou

4. Uplatnenie princípu partnerstva pri príprave zámeru národného projektu

Navrhovaný projekt bude organizačne a administratívne zabezpečený z vlastných kapacít z radov zamestnancov MIRRI SR a vzhľadom na uvedené nebude aplikované ustanovenie § 3, písm. t) zákona č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Popis národného projektu

5. Východiskový stav

a) Uveďte východiskové dokumenty na regionálnej, národnej a európskej úrovni, ktoré priamo súvisia s realizáciou NP:

Rozsah projektu, jeho ciele a prínosy sú v súlade s nasledujúcimi strategickými dokumentmi: Vízia a stratégia rozvoja Slovenska do roku 2030 a Stratégia digitálnej transformácie Slovenska 2030, ktorých cieľom je aj zvyšovanie dôveryhodnosti služieb štátu, budovanie bezpečnosti a odolnosti.

Ministerstvo investícií, regionálneho rozvoja a informatizácie ako orgán vedenia v oblasti informatizácie a zriaďovateľ vládnej jednotky CSIRT pre podsektor informačné systémy verejnej správy predkladaným projektom reaguje na celkovú úroveň kybernetickej bezpečnosti v podsektore. V zmysle zákona č.69/2018 Z.z. o kybernetickej bezpečnosti, je každá obec prevádzkovateľom základnej služby štátu a je povinná dodržiavať bezpečnostné opatrenia. Sú to úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie zákonom požadovanej úrovne kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov a operačných technológií.

Zároveň je potrebné konštatovať, že na obce do 6 000 obyvateľov sa vzťahujú bezpečnostné opatrenia Kategórie I. podľa zákona č.69/2018 Z.z.

Popis aktivít na obci je koncipovaný, ako minimálny balík, ktorý zabezpečí obci splnenie zákonných požiadaviek kategórie I podľa zákona č. 69/2018 Z. z..

V rozsahu 1,5 človekodňa na jednu obec budú realizované predovšetkým požadované služby, ktoré zabezpečia základné splnenie legislatívnych požiadaviek a základný technologický a procesný rámec kybernetickej a informačnej bezpečnosti. Jedná sa o kombináciu odbornej analytickej, implementačnej a vzdelávacej činnosti, ktorú vykoná zdieľaný manažér KIB.

b) Uveďte predchádzajúce výstupy z dostupných analýz, na ktoré nadväzuje navrhovaný zámer NP (štatistiky, analýzy, štúdie,...):

Kybernetická bezpečnosť na samosprávach je zanedbávaná a zriaďovatelia si neuvedomujú jej dôležitosť. Túto skutočnosť potvrdzuje aj správa o kybernetickej bezpečnosti v Slovenskej republike z roku 2023, kde v sektore verejná správa sa stav kybernetickej bezpečnosti dlhodobo nemení aj napriek veľkému počtu prevádzkovateľov. V danej správe vládna jednotka CSIRT v roku 2023 zaznamenala 1 012 incidentov, čo oproti minulému roku je nemenné číslo. Najviac hlásení o incidentoch pochádza zo sektorov verejná správa (478), bankovníctvo (77) a zdravotníctvo (26). Dominovali technické typy útokov, ako sú získavanie informácií, nedostupnosť, prienik do systému, škodlivý kód a zraniteľnosť.

Tento nález je v súlade so správou ENISA (European Union Agency for Cybersecurity) o hrozbách patria podobne ako v roku 2023 verejná správa a štátne inštitúcie najviac preferované hacktivistami. Verejná správa sú pre nich atraktívne ciele, pretože ich útoky môžu mať veľký dopad na spoločnosť a pritiahnuť pozornosť verejnosti.

c) Popíšte problémové a prioritné oblasti, ktoré rieši zámer NP. (Zoznam známych problémov, ktoré vyplývajú zo súčasného stavu a je potrebné ich riešiť):

Na základe údajov zo správy ENISA je najzasahovanejším cieľovým sektorom verejná správa pričom podľa správy NBÚ sú najviac používané typy útokov tzv. Phishingy (phishing je forma kybernetického útoku, kde sa útočník často vydáva za dôveryhodnú osobu aby získal osobné údaje, heslá a pod.). S prihliadnutím na uvedené bola zostavená ponuka technológií a služieb poskytovaná projektom tak, aby sme postupne eliminovali uvedené najslabšie miesta z pohľadu jednotlivých hrozieb.

V zásade ide o opatrenia, ktoré majú za cieľ minimalizovať riziko vzniku negatívnej udalosti, akými sú napríklad:

- Narušenie prevádzky siete alebo informačného systému, ktoré ohrozí integritu alebo dôvernosť spracovávaných osobných údajov,
- úniku osobných údajov v dôsledku čoho môže vzniknúť škoda na zdraví, či ujma na majetku,
- obmedzenie výkonu, alebo ohrozenie pôsobnosti obce, najmä s ohľadom na schopnosť zabezpečenia bezpečia, verejného poriadku alebo zvládnutia mimoriadnej udalosti.

Zároveň s narastajúcou digitalizáciou verejných služieb je dôležité, aby verejnosť mala dôveru v to, že ich údaje sú bezpečné a chránené. V súčasnom digitálnom prostredí, v ktorom sa významná časť kritických informácií a transakcií presúva do online sféry, sa vytvára potreba osobitného dôrazu na zachovanie dôvery medzi verejnosťou a verejnými inštitúciami.

Celkovo, integrovaním týchto bezpečnostných mechanizmov nejde len o technologický rozmer. Ide o kľúčový krok v procese budovania a posilňovania dôvery medzi verejnosťou a orgánmi verejnej správy. Tento krok zabezpečuje, že každý občan môže s istotou veriť, že jeho osobné údaje sú uchránené, a že verejné služby sú dostupné v každom momente, kedy sú potrebné.

d) Uveďte, na ktoré z ukončených a prebiehajúcich národných projektov[10] zámer NP priamo nadväzuje, v čom je navrhovaný NP od nich odlišný, resp. na ktoré NP čiastočne nadväzuje / prelína sa s nimi v istej časti a ako sú v ňom zohľadnené (čiastkové) výsledky/dopady predchádzajúcich NP (ak je to relevantné):

V rámci programového obdobia rokov 2014-2020 nebol realizovaný národný projekt smerovaný na podporu riešenia problematiky kybernetickej a informačnej bezpečnosti zameraný na obce do 6 000 obyvateľov.

e) Popíšte administratívnu, finančnú a prevádzkovú kapacitu žiadateľa a partnera (v prípade, ak je v projekte zapojený aj partner):

Administratívna a prevádzková kapacita v rámci projektu bude zabezpečená z vlastných kapacít zamestnancov MIRRI SR.

[10] V prípade, ak je to relevantné, uveďte aj ukončené národné projekty z programového obdobia 2014 – 2020.

Spolufinancovaný Európskou úniou

6. Hlavné ciele NP (stručne):

Hlavným cieľom projektu je zvýšene a zlepšenie úrovne kybernetickej a informačnej bezpečnosti v prostredí samosprávy do 6 000 obyvateľov. Tento cieľ plánujeme zrealizovať pomocou daných riešení:

- zavedením funkčných procesov riadenia rizík kybernetickej bezpečnosti
- vypracovaním dlhodobej bezpečnostnej stratégie, ktorá bude zahŕňať ciele, priority a konkrétne opatrenia na zlepšenie bezpečnosti
- zasadením pokročilých bezpečnostných technológií, ako sú EDR (Endpoint Detection and Response), firewall, NAS
- organizáciou pravidelných školení pre zamestnancov obecných úradov na zvýšenie ich povedomia a znalostí v oblasti kybernetickej bezpečnosti
- vytvorením vzdelávacích materiálov a online kurzov, ktoré budú dostupné pre všetkých zamestnancov
- zavedením systémov na neustále monitorovanie bezpečnostných incidentov a hrozieb
- vytvorením a implementáciou plánov reakcie na bezpečnostné incidenty, vrátane postupov na rýchlu obnovu systémov a dát
- zabezpečením efektívnej komunikácie medzi obcami, centrálnymi orgánmi a externými partnermi
- pravidelnou aktualizáciou bezpečnostných opatrení a politík na základe získaných poznatkov a skúseností.

Podľa § 5 ods. 2 písm. c) zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov, je obec orgánom riadenia a zároveň aj správcom informačných technológií vo verejnej správe. Do registra prevádzkovateľov základnej služby sa podľa § 17 ods. 1 písm. g) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, zapisuje každý správca informačných technológií vo verejnej správe. Ako poskytovatelia základných služieb štátu, sú obce povinné zabezpečiť kybernetickú bezpečnosť podľa požiadaviek definovaných v príslušnej legislatíve. Prostredníctvom tohto projektu sa obciam umožní dosiahnuť požadovaná úroveň kybernetickej a informačnej bezpečnosti s platnou legislatívou v podobe procesného, technického, hardvérového vybavenia, aplikácií, SW, ako aj zastrešenie zdieľanej funkcie IT security experta pre kybernetickú bezpečnosť.

Prínosy projektu budú smerované na plošné dosiahnutie a zjednotenie požadovaných štandardov v súlade s legislatívou v oblasti kybernetickej a informačnej bezpečnosti v podmienkach obcí a projekt posilní ochranu obcí technickými a organizačnými opatreniami pred narastajúcimi kybernetickými hrozbami.

7. Merateľné ukazovatele NP a iné údaje

Zoznam merateľných ukazovateľov projektu

Typ merateľného ukazovateľa projektu	Kód merateľného	Názov merateľného ukazovateľa projektu	Merná jednotka merateľného ukazovateľa projektu	Indikatívna cieľová hodnota[12]

[12] V zmysle zmluvy o poskytnutí nenávratného finančného príspevku sa pre typ merateľného ukazovateľa projektu – výstup štandardne cieľová hodnota nastavuje ku koncu realizácie národného projektu. Pre typ merateľného ukazovateľa projektu – výsledok sa štandardne cieľová hodnota nastavuje na obdobie udržateľnosti národného projektu.

	ukazovateľa projektu[11]			
výstup	PSKPSOI12	Verejné inštitúcie podporované v rozvoji kybernetických služieb, produktov a procesov	Verejné inštitúcie	1500
výsledok	PSKPRCR11	Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov	používatelia / rok	1500

Vysvetlenie merateľného ukazovateľa projektu „výstup“: Ako poskytovatelia základných služieb štátu, sú obce povinné zabezpečiť kybernetickú bezpečnosť podľa požiadaviek definovaných v príslušnej legislatíve. Vo väčšine obcí s počtom obyvateľov do 6 000 je však táto problematika často zanedbávaná a je na pokraji záujmu obce. Na Slovensku je aktuálne v uvedenej veľkostnej kategórii 2795 obcí (na základe počtu obyvateľov na konci roka 2023). Naplnením cieľa projektu by sa tak kybernetická bezpečnosť zvýšila celkovo v prípade 54 % obcí. Výška cieľovej hodnoty 1500 bola zvolená na základe časového a finančného rámca pre úspešné naplnenie cieľa so zachovaním kvality dodaných služieb.

Vysvetlenie merateľného ukazovateľa projektu „výsledok“: Indikatívna cieľová hodnota 1500 používateľov je určená na základe požiadaviek zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov, kde obec je orgánom riadenia a zároveň aj správcom informačných technológií vo verejnej správe. Z toho vyplýva že zodpovednou osobou za kybernetickú bezpečnosť obce je štatutár, ktorým je v tomto prípade starosta obce, t.j. používateľ.

Zoznam iných údajov projektu (ak relevantné)

Kód iného údaja[13]	Názov iného údaja	Merná jednotka iného údaja
DPSK034	Priemerná hrubá mesačná mzda financovaná z projektu za rok	EUR/rok
DPSK035	Medián priemerných hrubých mesačných miezd financovaných z projektu za rok	EUR/rok
DPSK033	Počet nástrojov zabezpečujúcich prístupnosť pre osoby so zdravotným postihnutím	počet

8. Prínosy, ktoré sa dajú očakávať pre cieľové skupiny (ak je to relevantné)

Cieľová skupina	Počet[14]	Prínos

[11] Uvádza sa kód merateľného ukazovateľa projektu, nie kód spoločného, resp. špecifického merateľného ukazovateľa programu. Ak merateľný ukazovateľ projektu ešte nemá pridelený kód, uvádza sa „n/a“.
[13] Ak iný údaj ešte nemá pridelený kód, uvádza sa „n/a“.
[14] Ak nie je možné uviesť početnosť cieľovej skupiny, uveďte do tejto časti zdôvodnenie.

Spolufinancovaný Európskou úniou

9. Aktivity národného projektu

a. V tabuľke nižšie uveďte rámcový popis aktivít, ktoré budú v rámci identifikovaného národného projektu realizované.

Názov aktivity	Čo sa má aktivitou dosiahnuť	Spôsob realizácie (žiadateľ a / alebo partner)	Predpokladaný počet mesiacov realizácie aktivity
Hlavná aktivita: Zvýšenie bezpečnostného štandardu v oblasti kybernetickej a informačnej bezpečnosti v podobe procesného, technického, hardvérového vybavenia, aplikácií, SW ako aj zastrešenie zdieľanej funkcie IT security experta pre kybernetickú bezpečnosť.	Zabezpečenie súladu z legislatívnymi požiadavkami, spracovanie bezpečnostnej dokumentácie, implementácia a zavedenie procesov, zdieľanie pozície IT security experta, inštalácia EDR, firewall, NAS a školenie pre štatutárov a zamestnancov	Žiadateľ (Realizácia pomocou dodávateľa, ktorý bude vyhlásený verejným obstarávaním.)	36

b. V tabuľke nižšie uveďte, či v rámci národného projektu bude uplatnený inštitút užívateľa[15] podľa § 3 písm. u) zákona č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Názov aktivity	Využitie inštitútu užívateľa (áno/nie)	Typ užívateľa[16]	Poskytovateľ príspevku užívateľovi (žiadateľ alebo partner)
Aktivita 1	nie		

V prípade viacerých aktivít, doplňte informácie za každú z nich.

c. Uveďte detailnejší popis aktivít.

Podaktivity projektu:

Technologické zvýšenie bezpečnosti

V prvej etape bude realizovaná implementácia hardvérových a softvérových riešení na základe vykonanej vstupnej GAP analýzy pre každú obec samostatne. Ďalej súčasťou prvej etapy bude aj pilotné overenie na vzorke obcí (max. 10), ktorého analytickým výstupom bude vypracovaná vzorová dokumentácia, ktorá sa bude upravovať a aktualizovať pre potreby každej obce. Nasadenie a inštalácia NAS, EDR a Firewall.

Postupný rollout na ďalšie obce na základe prejaveného záujmu obcí. Platforma Centrálny portál kybernetickej bezpečnosti ďalej nazývaný ako „kyberportál“, bude slúžiť ako hlavný komunikačný nástroj ohľadom možnej participácie obcí na projekte (nahlasovanie sa do databázy

[15] Užívateľ sa na rozdiel od partnera nepodieľa na realizácii projektu žiadateľa, ale môže využiť finančný príspevok na realizáciu aktivít definovaných poskytovateľom vo výzve (napr. nákup a inštalácia kotla). Podľa § 3 písm. u) zákona č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, užívateľom je osoba, ktorej prijímateľ alebo partner poskytuje finančné prostriedky z príspevku na základe predchádzajúceho súhlasu poskytovateľa a v súlade so zmluvou uzavretou medzi prijímateľom a užívateľom alebo partnerom a užívateľom alebo iným obdobným právnym vzťahom medzi prijímateľom a užívateľom alebo partnerom a užívateľom.

[16] Uvádza sa typ subjektu/osôb (napr. neverejní poskytovatelia soc. služieb, dlhodobí uchádzači o zamestnanie), alebo právna forma.

žiadateľov, zasielanie dokumentácie/informácie o AS IS stave obce z pohľadu KB, atď.). Obce si cez katalóg služieb v kyberportáli vyberú záujem o službu (NAS, EDR, Firewall, školenie zamestnancov, konzultačné služby kybernetickej a informačnej bezpečnosti experta, podpora pri implementácii dokumentácií kybernetickej bezpečnosti, dispečing). Vzhľadom na to, že predmetom dodávky projektu sú technológie a služby medzi poskytovateľom a obcou bude uzavretá vzájomná zmluva o zápožičke investičného majetku. HW, SW a licencie budú vo vlastníctve MIRRI SR. Bezpečnostná dokumentácia bude v majetku obce. Z tohto vyplýva, že obec nebude znášať náklady spojené s technickou podporou HW a SW dodaných licencií. Náklady spojené s podporou a predlžovaním licencií bude v rámci udržateľnosti projektu znášať MIRRI.

Zodpovednosť za poskytnuté HW, SW a licencie z pohľadu fyzickej bezpečnosti bude upravená v zmluvách o výpožičke kde bude uvedený zoznam zariadení, ktoré budú slúžiť na výkon kybernetickej bezpečnosti v obci a povinnosti obce pri ich prevádzke. Detailné požiadavky na fyzickú bezpečnosť HW/SW budú zahrnuté v technických požiadavkách opisu predmetu zákazky.

Dispečing je kľúčový systém podpory počas realizačnej a prevádzkovej fázy projektu, primárne je určený na harmonizovanie zavádzaných bezpečnostných technológií služieb a procesov. Dispečing a podpora L1 a L2 incidentov zabezpečuje dodávateľ. Podpora L3 incidentov zabezpečuje MIRRI SR prostredníctvom národného Systému včasného varovania (EWS).

Zabezpečenie súladu s legislatívnymi požiadavkami

Táto aktivita bude zameraná na zistenie stavu bezpečnostných opatrení pomocou checklistu pre subjekty kategórie I podľa vyhlášky č. 179/2020 Z.z. Celkovo ide o systematický prístup k hodnoteniu a zlepšovaniu bezpečnosti IT systémov pomocou kontrolného zoznamu a analýzy rozdielov. Zistenie stavu bezpečnostných opatrení na pomocou checklistu, základný stav bezpečnosti IT systémov a GAP analýza.

Spracovanie bezpečnostnej dokumentácie v súlade s požiadavkami zákona č. 95/2019 ZoITVS a zákona č. 69/2018 ZoKB. V rámci bezpečnostnej dokumentácie budú pre obce spracované aj interné smernice, ktoré súvisia s riadením KIB.

Implementácia zavedenia procesov a organizácie kybernetickej bezpečnosti. Celkovo ide o to, aby organizácia mala jasne definované a efektívne fungujúce mechanizmy na ochranu svojich informačných systémov a dát pred kybernetickými hrozbami.

Zdieľanie pozície IT security experta pre kybernetickú bezpečnosť. Celkovo teda ide o to, že jeden IT bezpečnostný expert bude poskytovať svoje služby viacerým organizáciám alebo oddeleniam, aby im pomohol zabezpečiť ich informačné systémy a dáta pred kybernetickými hrozbami.

Deliacou líniou sa rozumie naplnenie obsahovej časti povinných dokumentov pre konkrétne obce, ktoré sú poskytovateľ základnej služby (ďalej ako „PZS“) a ako základ tvoria normovane dokumenty vypracovane a odsúhlasene v rámci aktivít Reformy 4 tykajúcich sa štandardizácie a metodického zjednotenia dokumentácie legislatívne požadovanej. Reforma 4 neposkytuje individuálne výstupy a neráta s diverzitou cieľových PZS.

Zvýšenie povedomia o kybernetických hrozbách

Oboznámenie s technológiami čo majú nainštalované (NAS, EDR, firewall).

Hlavnou náplňou školenia, bude implementácia a podrobné vysvetlenie pravidiel a princípov obsiahnutých v bezpečnostnej dokumentácii, ktoré je potrebne dodržiavať pri dennom výkone činnosti na každej obci v spolupráci s manažérom kybernetickej bezpečnosti. Zároveň školenie bude vychádzať aj s bezpečnostnej dokumentácie vytvorenej pre každú obec samostatne so zohľadnením najmä na

základy kybernetickej bezpečnosti, phishingové útoky, bezpečné používanie hesiel a oboznámenie zamestnancov so základnými zásadami z pohľadu KB.

Zamestnanci obcí zodpovední za KB získajú prístup do implementovaných bezpečnostných nástrojov za účelom riešenia KIB incidentov. Tieto osoby budú mať možnosť absolvovať školenia k správe implementovaných bezpečnostných nástrojov.

Deliacou líniou voči "NP Vzdelávanie – Zvýšenie úrovne odbornosti v oblasti kybernetickej a informačnej bezpečnosti u zamestnancov verejne správy" je, že školenia v rámci predkladaného projektu budú vypracované na základe bezpečnostnej dokumentácie a dodávaného softvéru a hardvéru a budú určené výhradne na používanie SW, HW a konkrétnej bezpečnostnej dokumentácie pre konkrétnu obec.

Celkový prínos pre obce do 6 000 obyvateľov bude plošné zvýšenie kybernetickej a informačnej bezpečnosti a kontinuity poskytovaných služieb.

NP bude realizovaný v súlade s horizontálnymi princípmi s povinnosťou dodržania súladu projektu s Chartou základných práv Európskej únie, rodovou rovnosťou, nediskrimináciou a prístupnosťou osôb so zdravotným postihnutím, ktoré sú definované v Partnerskej dohode SR na roky 2021 – 2027 a v čl. 9 nariadenie o spoločných ustanoveniach, berúc do úvahy Chartu základných práv Európskej únie a povinnosti vyplývajúce z Dohovoru OSN o právach osôb so zdravotným postihnutím a zabezpečenia prístupnosti v súlade s jeho článkom 9, ako horizontálne základné podmienky. Pri implementácii plánovaných aktivít projektu sa budú dodržiavať všetky články Charty ZP EÚ s dôrazom najmä na články Charty ZP EÚ, ktoré sa najviac vzťahujú k plánovaným intervenciám, aktivitám a cieľovým skupinám.

V súvislosti so všetkými plánovanými aktivitami bude zohľadnený v rámci NP:

- princíp rovnosti mužov a žien a princíp nediskriminácie tak, aby nedochádzalo k znevýhodneným podmienkam pre akúkoľvek skupinu osôb a aby boli vytvorené podmienky prístupnosti aj pre osoby so zdravotným postihnutím k fyzickému prostrediu, k informáciám a komunikácii vrátane informačných a komunikačných technológií a systémov, ako aj k ďalším prostriedkom a službám dostupným alebo poskytovaným verejnosti.

10. Predpokladaný časový rámec

Predpokladaný dátum vyhlásenia výzvy vo formáte mesiac/rok	11/2025
Predpokladaná doba realizácie NP v mesiacoch	36

11. Finančný rámec[17]

a) žiadateľa

Fond	Európsky fond regionálneho rozvoja	
Celkové oprávnené výdavky NP podľa kategórie regiónu[18] (v EUR)	menej rozvinutý región	10 362 882
	viac rozvinutý región	3 070 981
Zdroj EÚ podľa kategórie regiónu[19] (v EUR)	menej rozvinutý región	8 808 449,7
	viac rozvinutý región	1 228 392,4
Zdroj ŠR podľa kategórie regiónu[20] (v EUR)	menej rozvinutý región	1 554 432,3
	viac rozvinutý región	1 842 588,6

[17] Finančný rámec je potrebné uvádzať za celý NP spolu a v prípade financovania NP z viacerých priorít/špecifických cieľov, aj v rozdelení podľa špecifických cieľov.
[18] V prípade Kohézneho fondu vyberte „neaplikuje sa“.
[19] V prípade Kohézneho fondu vyberte „neaplikuje sa“.
[20] V prípade Kohézneho fondu vyberte „neaplikuje sa“.

Vlastné zdroje prijímateľa[21] podľa kategórie regiónu[22] (v EUR)	Vyberte položku.	
	Vyberte položku.	
Miera spolufinancovania (v %)	Zdroj EÚ	74,71 %
	Štátny rozpočet SR	25,29 %
	Prijímateľ	0,00 %
Uplatňovanie špecifického pravidla financovania[23] (ak relevantné)		
Zdroj pro-rata (v %)	Vyberte položku.	
	Vyberte položku.	
V prípade uplatňovania systému pro-rata uveďte spôsob jeho stanovenia (pomer medzi VRR a MRR), ktorý sa uplatňuje v prípade realizácie operácií s prínosom pre oba kategórie regiónov, vrátane názvu dokumentu v akom bol stanovený.	V zmysle čl. 63 ods. 3 prvá veta Nariadenia Európskeho parlamentu a Rady (EÚ) 2021/1060 z 24. júna 2021, v projekte, ktorý zahŕňa/má prínos pre viac ako jednu kategóriu regiónu podľa článku 108 ods. 2 nariadenia o spoločných ustanoveniach v rámci členského štátu, sa výdavky spojené s projektom pridelia na príslušné kategórie regiónu na pomernom základe, a to podľa objektívnych kritérií. Objektívnym kritériom vzhľadom na povahu a zameranie projektu je podiel **zamestnancov verejnej správy** v bratislavskom regióne (NUTS II) k zamestnancom verejnej správy v SR (referenčným obdobím je rok 2021). Celkové oprávnené výdavky sa rozdelia nasledujúcim pomerom podľa kategórie regiónu: - pre menej rozvinutý región: 77,14 %, - pre viac rozvinutý región: 22,86 %.	

b) partnera (ak relevantné)

Fond	Vyberte položku.	
Celkové oprávnené výdavky NP podľa kategórie regiónu[24] (v EUR)	Vyberte položku.	
	Vyberte položku.	
Zdroj EÚ podľa kategórie regiónu[25] (v EUR)	Vyberte položku.	
	Vyberte položku.	
Zdroj ŠR podľa kategórie regiónu[26] (v EUR)	Vyberte položku.	
	Vyberte položku.	
Vlastné zdroje partnera[27] podľa kategórie regiónu[28] (v EUR)	Vyberte položku.	
	Vyberte položku.	
Miera spolufinancovania (v %)	Zdroj EÚ	
	Štátny rozpočet SR	
	Partner	
Zdroj pro-rata (v %)	Vyberte položku.	

[21] Uveďte v súlade so Stratégiou financovania Európskeho fondu regionálneho rozvoja, Európskeho sociálneho fondu plus, Kohézneho fondu, Fondu na spravodlivú transformáciu a Európskeho námorného, rybolovného a akvakultúrneho fondu na programové obdobie 2021 – 2027

[22] V prípade Kohézneho fondu vyberte „neaplikuje sa“.

[23] Uveďte konkrétne číslo tabuľky a jej názvu podľa Stratégie financovania Európskeho fondu regionálneho rozvoja, Európskeho sociálneho fondu plus, Kohézneho fondu, Fondu na spravodlivú transformáciu a Európskeho námorného, rybolovného a akvakultúrneho fondu na programové obdobie 2021 – 2027.

[24] V prípade Kohézneho fondu vyberte „neaplikuje sa“.

[25] V prípade Kohézneho fondu vyberte „neaplikuje sa“.

[26] V prípade Kohézneho fondu vyberte „neaplikuje sa“.

[27] Uveďte v súlade so Stratégiou financovania Európskeho fondu regionálneho rozvoja, Európskeho sociálneho fondu plus, Kohézneho fondu, Fondu na spravodlivú transformáciu a Európskeho námorného, rybolovného a akvakultúrneho fondu na programové obdobie 2021 – 2027

[28] V prípade Kohézneho fondu vyberte „neaplikuje sa“.

	Vyberte položku.	
V prípade uplatňovania systému pro-rata uveďte spôsob jeho stanovenia (pomer medzi VRR a MRR), ktorý sa uplatňuje v prípade realizácie operácií s prínosom pre oba kategórie regiónov, vrátane názvu dokumentu v akom bol stanovený.		

12.Rozpočet

Indikatívna výška finančných prostriedkov určených na realizáciu národného projektu a ich výstižné zdôvodnenie

Predpokladané finančné prostriedky na aktivity NP	Celkové oprávnené výdavky (v EUR)	Plánované vecné vymedzenie
Hlavné aktivity		
Aktivita 1		
013 - Softvér	3 665 334	Výdavky pozostávajú z priemerných ponúk od dodávateľov na implementáciu, konfiguráciu a dodanie riešenia pre EDR a centrálny zber udalostí vrátane licencií +suma externých prác.
022 Hardvér	3 428 215	Výdavky pozostávajú z priemerných ponúk od dodávateľov na implementáciu, konfiguráciu pre firewall a NAS, prepočítané na najvyšší počet zapojených obcí 1 500.
518 – Ostatné služby	5 034 224	Suma predstavuje školenia spojené s dodanými zariadeniami a softvérom, dispečing (L1, L2 podpora), zdieľaný manažér kybernetickej bezpečnosti.
521 Mzdové výdavky	427 240	Suma predstavuje súčet interných prác, ktoré pozostávajú z 9 rôznych pozícií (BC/CBA), ktoré zároveň nepredstavujú plné FTE. V prepočte na 36 mesiacov to predstavuje ekvivalent 4 FTE s priemernou mzdou 5 700 EUR v super hrubej mzde (celkové náklady zamestnávateľa.
Hlavné aktivity spolu	12 555 013	
Podporné aktivity		
907 Paušálna sadzba na nepriame výdavky	878 850	Paušálne výdavky Výška je stanovená prostredníctvom zjednodušeného vykazovania výdavkov. V rámci projektu predpokladáme rozpočtovanie paušálnych výdavkov na podporné činnosti vo výške 7% z oprávnených priamych nákladov projektu.
Podporné aktivity SPOLU	878 850	
CELKOM	13 433 863	

V prípade zvýšenia celkových oprávnených výdavkov NP (po jeho schválení komisiou pri Monitorovacom výbore pre Program Slovensko 2021 – 2027) o viac ako 15 % (a nejde o prípad, kedy je určenie alokácie výsledkom realizovanej štúdie uskutočniteľnosti), riadiaci orgán / sprostredkovateľský orgán predloží pred vyhlásením výzvy na schválenie príslušnej komisii pri Monitorovacom výbore pre Program Slovensko 2021 – 2027 upravený zámer NP.

Ostatné zmeny v rozpočte projektu (napr. doplnenie novej skupiny výdavkov, vypustenie skupiny výdavkov, zvýšenie alebo zníženie výšky oprávnených výdavkov v rámci skupín výdavkov a pod.) nie je potrebné predkladať na schválenie príslušnej komisii pri Monitorovacom výbore pre Program Slovensko 2021 – 2027.

13.Ďalšie informácie o národnom projekte

Cieľom projektu je systematické riešenie a eliminácia akumulovaného investičného dlhu v oblasti kybernetickej a informačnej bezpečnosti na úrovni obcí, pričom ambíciou je v maximálnej možnej miere znížiť náklady obcí spojené s implementáciou a prevádzkou bezpečnostných opatrení. Po uplynutí realizačnej a dokončovacej fázy projektu budú aktivity projektu financované z rozpočtu realizátora projektu, teda MIRRI SR ako súčasť udržateľnosti projektu. Počas doby udržateľnosti bude pripravený mechanizmus na dlhodobé poskytovanie centralizovaných služieb kybernetickej bezpečnosti pre obce v súlade s plánovanou reformou systému miestnych samospráv, ktorej cieľom by malo byť znižovanie počtu obcí, resp. úradov.

V rámci realizácie projektu bude podpísané memorandum o spolupráci so združením DEUS s cieľom zefektívniť poskytovanie služieb zapojeným obciam a využiť synergie aktivít združenia DEUS a MIRRI SR. Počas realizácie projektu zároveň bude vykonané zmapovanie osôb zodpovedných za bezpečnosť na jednotlivých obciach z dôvodu možnosti dlhodobej spolupráce. Okrem toho budú navrhnuté aj spôsoby zapojenia týchto osôb do projektu.

Plán testovania implementovaných nástrojov bude predmetom PID a DNR. Testovanie je plánované počas implementácie každého nasadeného nastroja podľa testovacích scenárov. Do testovania bude zapojená VJ CSIRT, ktorá po nasadení technológii vykoná test správnosti nastavenia politík zvonka pomocou systému Achiles aj z vnútra obce.

Detailnejšie informácie ohľadom národného projektu sú dostupné v linku nižšie. Daný link je odkaz na Metainformačný systém Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky kde sa nachádza kompletná dokumentácia v súlade s Vyhláškou 401/2023 Z.z.

Detail položky Projekt rozvoja IT, Kybernetická bezpečnosť v samospráve do 6 000 obyvateľov | MetaIS