MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

sekcia informačných technológií verejnej správy
odbor stratégie ITVS
Pribinova 25
811 09 Bratislava

Ministerstvo investícií, regionálneho rozvoja
a informatizácie SR
PhDr. JUDr. Mgr. Ervín Šimko, MSc.,
MBA, LL.M.,
generálny riaditeľ sekcie
kybernetickej bezpečnosti
Pribinova 25
811 09 Bratislava

Váš list číslo/zo dňa	Naše číslo	Vybavuje/referent	Bratislava
	020844/2025/oPMHIT-1	Ing. Lucia Lelkes	21.05.2025

Stanovisko Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej len „MIRRI“) ako orgánu vedenia v zmysle zákona č. 95/2019 Z.z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „zákon“), k projektu „Kybernetická bezpečnosť v samospráve do 6 000 obyvateľov“

V nadväznosti na Vami predložený projekt a zaevidovanú požadovanú projektovú dokumentáciu v zmysle vyhlášky 401/2023 Z.z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy (ďalej len „vyhláška“) v centrálnom metainformačnom systéme verejnej správy pre projekt_3351 s názvom: „Kybernetická bezpečnosť v samospráve do 6 000 obyvateľov“, v celkovej hodnote 13 433 863,84 € s DPH, si Vám na základe posúdenia predloženej projektovej dokumentácie, v zmysle zákona, dovoľujeme zaslať

súhlasné stanovisko.

Predložená projektová dokumentácia spĺňa všetky nevyhnutné náležitosti v zmysle vyhlášky a obsahuje jednoznačný popis navrhovaného riešenia. Vyhodnotenie splnenia podmienok pre udelenie súhlasného stanoviska je uvedené v prílohe č.1.

S pozdravom

Ing. et Ing. Martin Déneši, PhD., MSc.
poverený riadením sekcie
informačných technológií verejnej správy
(podpísané elektronicky podľa zákona č. 272/2016 Z. z.
v znení neskorších predpisov)

Príloha

Príloha č. 1 k Stanovisku k projektu

+421 2 20 92 8269 lucia.lelkes@mirri.gov.sk www.mirri.gov.sk

Príloha č.1 k Stanovisku k projektu

Názov projektu:	**Kybernetická bezpečnosť v samospráve do 6 000 obyvateľov**		
Žiadateľ:	**Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky**		
Výzva:			
Schválená projektová dokumentácia	**Názov**	**Verzia dokumentácie**	**Zo dňa**
	Projektový zámer		*16.05.2025*
	Prístup k projektu		*09.05.2025*
	BC/CBA		*09.05.2025*
	Zoznam rizík a závislostí		*14.03.2025*

Oblasť hodnotenia	**Hodnotenie MIRRI** (*ÁNO/NIE/ NERELEVANTNÉ*)	**Podmienka k oblasti hodnotenia** *Zdôvodnenie hodnotenia*
Projektový zámer - Manažérske zhrnutie	**ÁNO**	**V projekte je jasne zadefinovaná príslušnosť k Programu Slovensko.** *Projekt bude realizovaný v rámci:* *Operačný program: Program Slovensko* *Priorita: 1P1. Veda, výskum a inovácie* *Špecifický cieľ: RSO1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy* *Hlavné aktivity projektu:* • *Analýza a dizajn* • *Obstaranie technológií pre obce NAS, Firewall a EDR.* • *Implementácia s poskytnutím služieb podpory* *Cieľom projektu je zvýšiť kybernetickú bezpečnosť na obciach pomocou procesného, technického, hardvérového vybavenie, aplikácií, softvéru ako ja zastrešenie zdieľanej funkcie IT security experta pre kybernetickú bezpečnosť, a to:* • *Umožniť dosiahnuť požadovanú úroveň kybernetickej bezpečnosti samospráv v súlade s platnou legislatívou podľa zákona č.69/2018.* • *Zvýšiť kybernetickú bezpečnosť obce a informovanosť o kybernetickej bezpečnosti.* • *Vzdelanosť pracovníkov ohľadom kybernetickej bezpečnosti.* • *Poskytovanie služieb (EDR, NAS, firewall, školenie zamestnancov, konzultačné služby kybernetickej a informačnej bezpečnosti experta, podpora pri implementácii dokumentácií kybernetickej bezpečnosti).*

Projektový zámer - Motivácia a rozsah projektu – súlad so strategickými dokumentami	**ÁNO**	**Projektový zámer obsahuje konkrétny popis súladu navrhovaného projektu s cieľmi relevantných strategických dokumentov.** **Projekt je v súlade s Národnou koncepciou informatizácie verejnej správy 2021 (ďalej len „NKIVS“) a vyhláškou Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 401/2023 Z. z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy (ďalej len „vyhláška“).** *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. 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.* *Zvýšená schopnosť detekcie a prevencie hrozieb znižuje riziko kybernetických incidentov a znefunkčnenia informačných systémov územnej samosprávy a poskytovaných služieb občanom a podnikateľom. Zvýšením úrovne kybernetickej bezpečnosti dôjde k skvalitneniu ochrany aktív a celkovej dôveryhodnosti občanov voči samospráve a jej službám.* *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 zaznamenal 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.*
Projektový zámer - Zainteresované strany	**ÁNO**	**Žiadateľ identifikoval jednotlivých aktérov projektu** *Ministerstvo investícií, regionálneho rozvoja a informatizácie SR, Národný bezpečnostný úrad SR, občan/podnikateľ, externí dodávatelia, úradník samosprávy.*
Projektový zámer - Ciele projektu a merateľné ukazovatele	**ÁNO**	**Projekt má kvantifikované relevantné ciele a merateľné ukazovatele projektu** **Projekt má zadefinované relevantné merateľné ukazovatele zo zoznamu stanovených projektových merateľných ukazovateľov Programu Slovensko** *Názov cieľa: Zvýšenie a zlepšenie úrovne kybernetickej a informačnej bezpečnosti v prostredí samosprávy* *Národná stratégia Kybernetickej bezpečnosti na roky 2021 – 2025:*

		4.1 Dôveryhodný štát pripravený na hrozby *4.4 Kybernetická bezpečnosť ako základná súčasť verejnej správy* *Merateľné ukazovatele:* - *Zvýšenie bezpečnostného štandardu v oblasti kybernetickej a informačnej bezpečnosti pre obce do 6.000 obyvateľov v podobe procesného, technického, hardvérového vybavenia, EDR, NAS, firewall, dokumentácia. (AS-IS 0; TO-BE 1500)* - *Počet obcí kde bude zavedené pravidelné skenovanie zraniteľnosti na koncových bodoch monitorovaných prostredníctvom EDR (AS-IS 0; TO-BE 1500)*
Projektový zámer - Špecifikácia potrieb koncového používateľa	**ÁNO**	**V projekte sú identifikované potreby koncového používateľa a bol zrealizovaný zákaznícky prieskum** *Vzhľadom na rozsah a charakter projektu bola riadenými rozhovormi potvrdená požiadavka na využitie Centrálneho portálu kybernetickej bezpečnosti ako hlavného komunikačného nástroja pre proces prihlasovania sa obcí do projektu, zdieľanie informácií pre potreby GAP analýzy a inej dokumentácie. Súčasná verzia portálu bola implementovaná za dodržania Jednotného dizajn manuálu pre tvorbu elektronických služieb a webových sídel ID-SK. Akékoľvek úpravy Centrálneho portálu kybernetickej bezpečnosti budú vykonané taktiež v súlade s dizajn manuálom. Identifikovaní koncoví používatelia sú zamestnanci a štatutári zapojených obcí. Pre proces onboardingu, zdieľania informácií a inej dokumentácie bude zmapovaná používateľská cesta.*
Projektový zámer - Riziká a závislosti	**ÁNO**	**Žiadateľ identifikoval a vyhodnotil riziká a závislostí** *Register rizík a závislostí je zverejnený v MetaIS:* https://metais.slovensko.sk/ci/Projekt/37a7b1e4-5095-4cc0-8b96-d662ee2f9a45/documents
Projektový zámer – Alternatívy a MCA	**ÁNO**	**V projekte sú identifikované alternatívy riešenia projektu a vykonaná MCA** *Predložený projekt nezahŕňa budovanie ani rozvoj informačných systémov verejnej správy (ISVS), alternatívy sa teda nehodnotili tradičným spôsobom podľa biznisovej architektúry. Namiesto toho sa porovnali štyri rôzne možnosti riešenia aktuálnej situácie. Na základe rozsahu problému, ktorý bol identifikovaný v projektovom zámere, boli stanovené štyri rôzne alternatívne riešenia, a to: 1. Zachovanie súčasného stavu bez realizácie projektu, 2. Kybernetická bezpečnosť realizovaná obcami samostatne (decentralizovane), 3. Realizácia Kybernetická bezpečnosť pre samosprávy SR do 6000 obyvateľov, 4. Centralizované Cloud riešenie pre NAS. Ako najefektívnejšie sa vybrala alternatíva č.3 (Realizácia Kybernetická bezpečnosť pre samosprávy SR do 6000 obyvateľov), ktorá komplexne pokrýva procesy a požiadavky všetkých zainteresovaných strán.*
	ÁNO	**V projekte bolo zvažované použitie SW s otvoreným zdrojovým kódom (open source)** *Uplatnenie open source riešení bolo v projekte zvažované, avšak vzhľadom na priamy súvis aplikačnej a technologickej vrstvy, kde aplikačnú vrstvu tvorí obslužný SW pre HW, resp. bezpečnostný charakter aplikačných nástrojov neboli*

		identifikované vhodné open source riešenia. V prípade, že v procese implementácie bude identifikovaný vhodný open source nástroj, bude jeho implementácia predmetom fázy analýza a dizajn.
Projektový zámer – Požadované výstupy	**ÁNO**	**Žiadateľ definoval požadované projektové výstupy a produkty** *Projekt bude pri implementácii postupovať v zmysle vyhlášky 401/2023 Z.z*
Projektový zámer – náhľad architektúry	**ÁNO**	**Žiadateľ popísal cieľový produkt projektu z pohľadu biznis/aplikačnej/technologickej architektúry** *Projektový zámer obsahuje stručný náhľad budúcej IT architektúry. Detailný pohľad na IT architektúru je predmetom dokumentu Prístup k projektu.*
Projektový zámer – Legislatíva	**NERELEVANTNÉ**	**Žiadateľ neidentifikoval zmeny v oblasti legislatívy potrebné pre naplnenie cieľov a dodanie výstupov projektu** *Projekt nepredpokladá potrebu legislatívnych zmien pre naplnenie cieľov a dodanie výstupov projektu, pričom budú dodržané východiská platnej legislatívy.*
Projektový zámer – Rozpočet a prínosy	**ÁNO**	**Žiadateľ popísal a vyčíslil indikatívne náklady a prínosy projektu** *Žiadateľ vyčíslil náklady projektu na 10 rokov dopredu, pričom vyčíslil a slovne popísal prínosy a rok návratnosti (ukazovatele: ENPV, FNPV, BCR).* *- Výška plánovaných ročných nákladov na prevádzku a rozvoj HW a SW spolu je 1 224 518 €* *- Rok návratnosti projektu je T6 a BCR má hodnotu 1,76.*
Projektový zámer – Harmonogram	**ÁNO**	**Žiadateľ spracoval detailný plánovaný harmonogram projektu, vrátane jednotlivých fáz projektu a identifikoval metódu jeho riadenia** *Projekt je nastavený na 36 mesiacov v rámci podporných aktivít* *- Finálny termín ukončenia realizačnej fázy projektu vrátane post implementačnej podpory projektu je 06/2026* *- Finálny termín ukončenia projektu je 07/2027* *- Projekt bude realizovaný metódou Waterfall, a to formou jedného inkrementu (inkrement tvoria 3 moduly)*
Projektový zámer – Projektový tím	**ÁNO**	**V Projektovom zámere je stanovené zloženie RV a projektového tímu**
Projektový zámer – Pracovné náplne	**ÁNO**	**V Projektovom zámere sú zadefinované rámcové pracovné náplne členov projektového tímu**
Projektová dokumentácia a evidenčná povinnosť v MetaIS	**ÁNO**	**Projektová dokumentácia pre prípravnú a iniciačnú fázu je vypracovaná v súlade s vyhláškou** *Všetky dokumenty vypracované počas realizácie projektu musia byť v súlade s vyhláškou 401/2023 Z.z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy a publikované v MetaIS* **Žiadateľ splnil evidenčnú povinnosť v zmysle zákona 95/2019 Z.z. o informačných technológiách vo verejnej správe, § 12 evidenčná povinnosť v MetaIS** *V MetaIS sú evidované všetky entity, ich atribúty a vzťahy*

		Projektová dokumentácia prešla verejným pripomienkovaním v termíne od 10.03. – 31.03.2025 v súlade s vyhláškou , §4 ods. 11. Pripomienky ako aj status o vysporiadaní je zverejnený v MetaIS.
Katalóg požiadaviek	**ÁNO**	**Žiadateľ vypracoval Katalóg požiadaviek, ktorý je súčasťou dokumentu BC/CBA** *Projekt obsahuje 30 funkčných, 174 nefunkčných požiadaviek.*
Prístup k projektu – Biznis vrstva	**ÁNO**	**Projekt podrobne popisuje súčasný stav a navrhované riešenie z pohľadu biznis architektúry** *Biznis architektúra AS IS stavu zobrazuje momentálny stav kybernetickej a informačnej bezpečnosti na obciach do 6000 obyvateľov, v súčasnom stave predstavujú prístupové miesta kyberportál a VISKB portál (Centrálny modul Vládneho informačného systému kybernetickej bezpečnosti). Biznis architektúra TO BE stavu reflektuje projektový zámer, ktorým je zvýšenie kybernetickej a informačnej bezpečnosti na obciach do 6000 obyvateľov.*
Prístup k projektu – Aplikačná vrstva	**ÁNO**	**Projekt podrobne popisuje súčasný stav a navrhované riešenie z pohľadu aplikačnej architektúry a sú identifikované a popísané plánované integrácie a prepojenia. Navrhované riešenie je v súlade so zákonom 305/2013 Z.z. o e-Governmente, § 10 spoločné moduly** (autentifikačný modul - IAM , modul elektronických formulárov – MEF, modul elektronických schránok – eDESK, modul procesnej integrácie a integrácie údajov – CPDI, platobný modul – MEP, modul elektronického doručovania – MED, modul centrálnej elektronickej podateľne – CEP) • *Model aplikačnej architektúry v stave AS-IS je možné len odhadnúť dôvodu veľkého počtu obcí, komplikovanosti a nerentabilnosti vykonania analýzy aktuálneho stavu na mieste. Vzhľadom na očakávanú chýbajúcu mieru povedomia kybernetickej bezpečnosti je možné predpokladať, že na obci je maximálne implementované antivírusové riešenie. Na obci sa nachádzajú informačné systémy obce, ktoré sú buď centralizované cez DEUS alebo lokálne inštalované na klientskych staniciach prípadne serveroch.* • *Vzhľadom na charakter projektu bude aplikačná architektúra v TO-BE stave doplnená o hardvérové komponenty firewall a úložiskom dát, ktoré budú umiestnené na lokalite obce. Aplikačné komponenty na lokalite obce budú priamo integrované v týchto hardvérových komponentoch a predstavujú ich obslužný softvér.*
Prístup k projektu – Dátová vrstva	**NERELEVANTNÉ**	**Projekt popisuje navrhované riešenie z pohľadu dátovej vrstvy a dátového rozsahu. Navrhované riešenie je v súlade so strategickou prioritou NKIVS otvorené údaje a s vyhláškou 78/2020 Z.z. o štandardoch pre informačné technológie verejnej správy, § 40 Poskytovanie otvorených údajov** *Dátová vrstva je vzhľadom na charakter a rozsah projektu nerelevantná. V rozsahu projektu neboli identifikované údaje použiteľné ako referenčné údaje, moje údaje, otvorené údaje alebo analytické údaje.*
Prístup k projektu – Technologická vrstva	**ÁNO**	**Projekt podrobne popisuje súčasný stav a navrhované riešenie z pohľadu technologickej architektúry. Navrhované riešenie je v súlade so strategickou prioritou NKIVS vládny cloud a zákonom 305/2013 Z.z. o e-Governmente, § 10a Vládny cloud** *Projekt je navrhnutý tak, aby postupne zvyšoval úroveň kybernetickej bezpečnosti v samosprávnom sektore. Pred zavedením nových technológií, ako sú firewally, systémy NAS (Network Attached Storage) a EDR (Endpoint Detection and Response), bude vykonaná dôkladná analýza existujúcich procesov a infraštruktúry každej obce. Táto analýza umožní*

		identifikovať konkrétne bezpečnostné medzery a navrhnúť optimalizované riešenia. Nové technológie budú implementované postupne, pričom dôraz bude kladený na ich integráciu do existujúcich procesov. Zamestnanci obcí budú preškolení v oblasti používania týchto nástrojov a získajú potrebné znalosti na efektívne reagovanie na bezpečnostné incidenty. Školenia budú zamerané na praktické aspekty, ako je napríklad správna konfigurácia zariadení, rozpoznávanie phishingových útokov a správanie sa v prípade podozrivých aktivít. Kombináciou týchto opatrení sa zabezpečí, že obce budú vybavené modernými nástrojmi na ochranu svojich dát a budú schopné proaktívne čeliť kybernetickým hrozbám. Systémy NAS zabezpečia bezpečnú a centralizovanú správu dát, firewally ochránia sieťové prenosy a EDR systémy umožnia včasnú detekciu a reakciu na bezpečnostné incidenty. Vďaka tomuto komplexnému prístupu sa zvýši odolnosť obcí voči kybernetickým útokom a zabezpečí sa kontinuita poskytovaných služieb. *Využívanie služieb z katalógu služieb vládneho cloudu: vzhľadom na charakter a rozsah projektu z oblasti kybernetickej bezpečnosti je daná časť nerelevantná. Vládny cloud neposkytuje predmetné služby v rámci katalógu služieb vládneho cloudu.*
Prístup k projektu – Bezpečnostná architektúra	**ÁNO**	**Projekt popisuje stav riešenia bezpečnostnej architektúry** *Bezpečnostná architektúra navrhnutá v rámci projektu je zameraná na vytvorenie národného prostredia, ktoré umožní efektívne zvyšovať úroveň kybernetickej bezpečnosti pre samosprávy a občanov Slovenskej republiky využívajúcich elektronické služby. Implementované riešenia budú v súlade s nasledujúcimi princípmi bezpečnej architektúry:* • *Obrana do hĺbky* • *Rozčlenenie* • *Princíp najmenších privilégií* • *Všetka komunikácia medzi bezpečnostnými nástrojmi a centrálnou časťou systému včasného varovania je zabezpečená.* • *Všetka komunikácia bude prebiehať najbezpečnejším dostupným spôsobom, chrániť dôvernosť a integritu.* • *Riadenie prístupu na základe rolí* • *Zoznamy riadenia prístupu* • *Všetky komponenty riešenia musia byť časovo synchronizované. Presná synchronizácia času je dôležitá pre bezpečnosť z pohľadu forénznych analýz.*
Prístup k projektu – Závislosti na ostatné IS/projekty	**NERELEVANTNÉ**	**Žiadateľ neidentifikoval projekty, ktoré sú v štádiu vývoja a v korelácii s projektom. Navrhované riešenie je v súlade so zákonom 305/2013 Z.z. o e-Governmente, § 25 , odsek (7) – verejne dostupné aplikačné rozhranie** *Projekt nie je pre dosiahnutie cieľov a merateľných ukazovateľov závislý na iných ISVS alebo projektoch.*
Prístup k projektu – Zdrojové kódy	**NERELEVANTNÉ**	**V projekte sú stanovené požiadavky na zdrojové kódy, spôsob ich preberania a spôsob archivácie. Navrhované riešenie je v súlade so zákonom 95/2019 Z.z. o o informačných technológiách vo verejnej správe, § 15, odsek (2) bod d) EUPL a zabránenie vendor – lock a vyhláškou 78/2020 Z.z. o štandardoch pre informačné technológie verejnej správy, § 31 Centrálny repozitár zdrojových kódov**

		Vzhľadom na charakter projektu nie je predpoklad vzniku zdrojových kódov – projekt z oblasti kybernetickej bezpečnosti je danú časť nerelevantný. V rozsahu projektu je plánovaný HW, SW pre HW ako krabicové riešenie od výrobcu. *V prípade, ak by súčasťou dodávky boli aj zdrojové kódy k vytvorenému riešeniu, pokiaľ to nevylučujú licenčné podmienky tretích osôb vo vzťahu k štandardným Softvérovým produktom, budú tieto dodané s komentármi a technickým popisom, a to pre prevádzkové a testovacie verzie počítačových programov, a práva na ich zverejnenie v centrálnom repozitári zdrojových kódov podľa § 15 ods. 2 písm. d) Zákona o informačných technológiách vo verejnej správe a § 31 vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu o štandardoch pre informačné technológie verejnej správy č. 78/2020 Z. z., a iného predpisu, ktorý môže v budúcnosti vyhlášku č. 78/2020 Z. z. nahradiť alebo doplniť.*
Prístup k projektu – Prevádzka a údržba	**ÁNO**	**V projekte sú stanovené požiadavky na prevádzku a dostupnosť budovaného/rozvíjaného ISVS** *Podpora prevádzky budovaných systémov bude realizovaná cez 3 úrovne podpory, s nasledujúcim označením:* • *L1 podpory IS (Level 1, priamy kontakt zákazníka) – zabezpečuje dodávateľ projektu cez dispečing* • *L2 podpory IS (Level 2, postúpenie požiadaviek od L1) – zabezpečuje dodávateľ projektu cez dispečing* • *L3 podpory IS (Level 3, postúpenie požiadaviek od L2) – zabezpečuje výrobca danej technológie cez platenú podporu* *Správa bezpečnostných incidentov:* • *L1 analytik (Level 1, priamy kontakt zákazníka) – zabezpečuje dodávateľ projektu cez dispečing* • *L2 analytik (Level 2, postúpenie požiadaviek od L1) – zabezpečuje dodávateľ projektu cez dispečing* • *L3 analytik (Level 3, postúpenie požiadaviek od L2) – zabezpečuje vládna jednotka CSIRT/NASES po zaškolený dodávateľom*
Prístup k projektu – Implementácia a preberanie výstupov	**ÁNO**	**V projekte sú stanovené požiadavky na implementáciu a preberanie výstupov projektu** *Projekt bude implementovaný v zmysle vyhlášky č. 401/2023 Z. z. o projektovom riadení bez rozdelení na viaceré inkrementy. Rozdelenie na inkrementy v projekte nie je možné vzhľadom na požiadavky inkrementu definovaných vyhláškou, podľa ktorých nie je možné realizovať viaceré inkrementy súbežne. Vzhľadom na charakter a rozsah projektu budú jednotlivé moduly, ktoré spolu vytvárajú jeden inkrement realizované paralelne v zmysle prístupu k implementácii jednotlivých častí projektu.*
BC/CBA (ekonomická analýza)	**ÁNO**	**Rozpočet projektu je 13 433 863,84 € s DPH.** *Projekt má vypracovaný položkový rozpočet v predpísanej štruktúrovanej forme, analýzu celkových nákladov na vlastníctvo a má vyhodnotenú ekonomickú a finančnú efektívnosť.*
Celkové hodnotenie projektu		**Schválenie projektu**

Doložka o autorizácii

Tento listinný rovnopis elektronického úradného dokumentu bol vyhotovený podľa vyhlášky č. 85/2018 Z. z. Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu z 12. marca 2018, ktorou sa ustanovujú podrobnosti o spôsobe vyhotovenia a náležitostiach listinného rovnopisu elektronického úradného dokumentu.

Údaje elektronického úradného dokumentu	
Názov:	[Národný projekt - Kybernetická bezpečnosť v samospráve do 6 000 obyvateľov - MIRRI]
Identifikátor:	020844/2025/oPMHIT-038809/2025

Autorizácia elektronického úradného dokumentu	
Dokument autorizoval:	"Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky" SK IČO: 50349287
Spôsob autorizácie:	kvalifikovaná elektronická pečať s pripojenou kvalifikovanou elektronickou časovou pečiatkou
Deklarovaný dátum a čas autorizácie:	23.05.2025 14:35:23 časové pásmo +02:00
Dátum a čas vystavenia kvalifikovanej časovej pečiatky:	23.05.2025 14:35:23 časové pásmo +02:00
Označenie listov, na ktoré sa autorizácia vzťahuje:	020844/2025/oPMHIT-038809/2025

Autorizácia prílohy elektronického úradného dokumentu	
Dokument autorizoval:	"Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky" SK IČO: 50349287
Spôsob autorizácie:	kvalifikovaná elektronická pečať s pripojenou kvalifikovanou elektronickou časovou pečiatkou
Deklarovaný dátum a čas autorizácie:	23.05.2025 14:35:29 časové pásmo +02:00
Dátum a čas vystavenia kvalifikovanej časovej pečiatky:	23.05.2025 14:35:29 časové pásmo +02:00
Označenie listov, na ktoré sa autorizácia vzťahuje:	020844/2025/oPMHIT-038809/2025-P001

Informácia o vyhotovení doložky o autorizácii	
Doložku vyhotovil:	Ing. Lucia Lelkes
Funkcia alebo pracovné zaradenie:	referent
Označenie orgánu verejnej moci:	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky IČO: 50349287
Dátum vytvorenia doložky:	23.05.2025
Podpis a pečiatka:	