Príloha č. 9 výzvy Minimálne obsahové a formálne náležitosti Deklarácie súladu

Žiadateľ je pre splnenie podmienky výzvy „Podmienka súladu Žiadosti o NFP s horizontálnou štúdiou uskutočniteľnosti a s minimálnymi obsahovými a formálnymi náležitosťami definovanými Prílohou č. 9 výzvy" a príslušného hodnotiaceho kritéria č. 2.1 „Je projekt v súlade s horizontálnou štúdiou uskutočniteľnosti, technickou špecifikáciou a získaným stanoviskom od ÚPVII z hľadiska minimálnych obsahových a formálnych náležitostí" **povinný vypracovať dokument Deklarácia súladu projektu s horizontálnou štúdiou uskutočniteľnosti pre dopytovú výzvu "Zvýšenie úrovne informačnej a kybernetickej bezpečnosti v podsektore ISVS / ITVS" (ďalej len Deklarácia súladu) (príloha č. 11 výzvy)** a podľa špecifikácie nižšie popísať požadované skutočnosti za účelom získania stanoviska od ÚPVII (SKB) k predmetnému projektu. **Hodnotiace kritéria pre dopytovo – orientované projekty „Zvýšenie úrovne informačnej a kybernetickej bezpečnosti v podsektore IS"** su zverejnené na stránke https://www.vicepremier.gov.sk/projekty/projekty-esif/operacny-program-integrovana-infrastruktura/prioritna-os-7-informacna-spolocnost/metodicke-dokumenty/hodnotiace-kriteria-op-ii/index.html.

	Kapitola/ obsah výzvy	*Odporúčaný max. počet slov*	*Obsahové a formálne náležitosti*
1	Popis projektu	500	Stručné manažérske zhrnutie by malo obsahovať zhrnutie dôležitých záverov z každej z nasledujúcich kapitol, pričom by malo ísť o súvislý logický text. Kapitola by mala obsahovať odpovede na otázky: Prečo robíme projekt? Čo je predmetom projektu? Pre koho sú výsledky projektu? Za akú sumu? Čo to prinesie cieľovej skupine?
3	Popis východiskovej situácie	600	Žiadateľ identifikuje naliehavosť situácie, z dôvodu ktorej vypracoval tento projekt. Situácia môže predstavovať problém, alebo príležitosť pre zlepšenie. Môže si pomôcť vyjadrením stavu / dopadu, ak by sa projekt nerealizoval. Môžu byť identifikované informačné systémy, ktorých sa projekt týka. Je potrebné uviesť informácie, ktoré pomôžu posúdiť prioritu projektu podľa hodnotiacich kritérií - požiadavka posúdenia hodnotiaceho kritéria 2.9 - priority predkladaného projektu s ohľadom na cieľové informačné systémy, nevyhnutnosť a relevantnosť riešení: A) Zistenie súčasného stavu KIB daného OVM na základe výsledkov penetračných testov a/alebo bezpečnostného auditu zrealizovaných vládnou jednotkou CSIRT, alebo nezávislým odborným subjektom, analýzy rizík a zaznamenaných kompromitácií v zmysle zákona č. 69/2018 Z. z. a zákona č. 95/2019 Z. z. a súvisiacich predpisov. Samotné výsledky môžu byť k dispozícii k nahliadnutiu. B) Ohodnotenie kritickosti informačných systémov daného OVM – či sa jedná o významný IS, resp. či ide o prvok kritickej infraštruktúry, ktorého kompromitácia by znamenala vážne následky na výkon štátnej správy. C) Ohodnotenie, či je cieľom projektu zabezpečiť daný OVM v jednej z týchto prioritných oblastí: 1) Zvýšenie ochrany pred útokmi z externého prostredia, 2) Zvýšenie schopnosti detekcie škodlivých aktivít a bezpečnostných incidentov 3) Ochrana dát, dátových prenosov a komunikácie, 4) Budovanie bezpečnostného povedomia. V súvislosti s hodnotiacimi kritériami 2.11, 2.12 a 2.14 je v tejto kapitole potrebné: 2.11. zdokumentovať výsledky analýzy rizík (vzhľadom na fakt, že ide o utajované alebo citlivé informácie, môžu byť výsledky analýzy rizík neverejné a prístupné len k nahliadnutiu), 2.12. zdokumentovať komplexný rámec riadenia bezpečnosti, stratégie, alebo opatrení kybernetickej bezpečnosti. V prípade citlivosti informácii je potrebné zdokumentovať existenciu týchto dokumentov, ich stručný popis a mať ich k dispozícii k nahliadnutiu. 2.14. zdokumentovať ako potreba navrhovaných nástrojov, resp. opatrení vyplýva z internej dokumentácie žiadateľa - kybernetickej stratégie, koncepcie, alebo politiky informačnej bezpečnosti žiadateľa, alebo z iných strategických a analytických dokumentov.
4	Spôsob realizácie aktivít projektu	500	Kapitola obsahuje zoznam aktivít a popis projektových činností, ktoré sa budú v týchto aktivitách realizovať. Povinnou aktivitou je Nákup HW a krabicového SW a podporné aktivity. Publicita a informovanosť musí obsahovať minimálne povinné položky (Umiestnenie trvalo vysvetľujúcej tabule a Dočasný veľkoplošný pútač). Popísať budúce riešenie základného rámca zabezpečenia informačnej a kybernetickej bezpečnosti sektorových OVM na úrovni biznis architektúry. Podľa horizontálnej štúdie uskutočniteľnosti môže pozostávať z nasledovných funkcií: • Kybernetická ochrana a detekcia škodlivých aktivít a bezpečnostných incidentov: • Bezpečnostný monitoring, pozostávajúci z nasledovných procesov: • monitoring IS, platforiem, aplikácií a používateľských činností a aktivít, • monitoring sietí, • monitoring činností a aktivít privilegovaných používateľov, • analýza založená na big-data a machine learning algoritmoch, • Riadenie bezpečnostných incidentov, pozostávajúce z nasledovných procesov: • identifikácia a hlásenie bezpečnostných incidentov, • registrácia, kategorizácia a klasifikácia bezpečnostných incidentov, • akceptácia bezpečnostných incidentov a určenie riešiteľov, • analýza a vyšetrovanie bezpečnostných incidentov a zber dôkazov. • riešenie bezpečnostných incidentov a obnova prevádzky, • uzatvorenie bezpečnostných incidentov, • vyhodnotenie bezpečnostných incidentov, zavedenie do KB DB, spätná väzba a poučenie sa z bezpečnostného incidentu. • Ochrana dát, dátových prenosov a komunikácie: • bezpečnosť virtualizovaných prostredí, • ochrana dát na úrovni databáz a dátových úložísk (šifrovanie dát), • ochrana dát na úrovni koncových zariadení (EPP - šifrovanie dát pri každom ich prenose alebo uchovávaní v lokálnom alebo centrálnom úložisku, kontrola a šifrovanie externých médií a pod.), • riadenie prístupov (implementácia nástrojov IAM a remote access manažmentu), • monitoring bezpečnosti na rozhraní s vyvedením logov do vládnej jednotky CSIRT. • proces bezpečnej výmeny citlivých informácií s vládnou jednotkou CSIRT, prípadne inými spolupracujúcimi OVM (integráciou na JISKB prostredníctvom vládnej jednotky CSIRT a
4	Situácia po realizácii projektu a udržateľnosť projektu	800	Kapitola obsahuje stručný popis budúceho stavu minimálne z aplikačného a technologického pohľadu. Súčasťou popisu by mal byť obrázok, kde budú zvýraznené nové prvky, ktoré sú dodávané projektom. V súvilosti s príslušnými hodnotiacimi kritériami je potrebné: 2.13. zdokumentovať rámcové technické riešenie na prepojenie rozhrania s vládnou jednotkou CSIRT, resp. Jednotným informačným systémom kybernetickej bezpečnosti (Toto kritérium sa posudzuje len v prípade, že projekt má za účel zriadiť systém na identifikáciu bezpečnostných incidentov. Ak projekt takýto systém nezriaďuje,nie je potrebné riešenie dokumentovať.) 3.3 žiadateľ musí zdokumentovať, že buď disponuje adekvátnym materiálno-technickým zázemím s dostatočnými internými administratívnymi kapacitami na zabezpečenie prevádzky projektu, alebo deklarovať čestným prehlásením, že kapacity zabezpečí prostredníctvom externého dodávateľa min. po dobu udržateľnosti projektu.

Podľa horizontálnej štúdie uskutočniteľnosti môže projekt riešiť nasledovné funkcie:
Kybernetická ochrana a detekcia škodlivých aktivít a bezpečnostných incidentov:
• Bezpečnostný monitoring, pozostávajúci z nasledovných procesov:
o monitoring IS, platforiem, aplikácií a používateľských činností a aktivít,
o monitoring sietí,
o monitoring činností a aktivít privilegovaných používateľov,
• analýza založená na big-data a machine learning algoritmoch,

Riadenie bezpečnostných incidentov, pozostávajúce z nasledovných procesov:
• identifikácia a hlásenie bezpečnostných incidentov,
• registrácia, kategorizácia a klasifikácia bezpečnostných incidentov,
• akceptácia bezpečnostných incidentov a určenie riešiteľov,
• analýza a vyšetrovanie bezpečnostných incidentov a zber dôkazov.
• riešenie bezpečnostných incidentov a obnova prevádzky,
• uzatvorenie bezpečnostných incidentov,
• vyhodnotenie bezpečnostných incidentov, zavedenie do KB DB, spätná väzba a poučenie sa z bezpečnostného incidentu.

Ochrana dát, dátových prenosov a komunikácie:
• bezpečnosť virtualizovaných prostredí,
• ochrana dát na úrovni databáz a dátových úložísk (šifrovanie dát),
• ochrana dát na úrovni koncových zariadení (EPP - šifrovanie dát pri každom ich prenose alebo uchovávaní v lokálnom alebo centrálnom úložisku, kontrola a šifrovanie externých médií a pod.),
• riadenie prístupov (implementácia nástrojov IAM a remote access manažmentu),
• monitoring bezpečnosti na rozhraní s vyvedením logov do vládnej jednotky CSIRT.
• proces bezpečnej výmeny citlivých informácií s vládnou jednotkou CSIRT, prípadne inými spolupracujúcimi OVM (integráciou na JISKB prostredníctvom vládnej jednotky CSIRT a implementovaním prostriedkov šifrovej ochrany informácií).
• riadenie SW záplat (Patch management).
• Zvýšenie ochrany pred útokmi z externého prostredia:
• ochrana pred malware a ransomware,
• manažment bezpečnosti sietí (nasadenie nových moderných sieťových prvkov /AFW, NGFW, a pod./),
• manažment bezpečnostných konfigurácií (implementácia systému pre jednotnú správu a deployment bezpečnostných politík a bezpečnostných konfigurácií),

Budovanie bezpečnostného povedomia a bezpečnostnej kultúry:
• výcvik a tréning a tréning zamestnancov v oblasti kybernetickej a informačnej bezpečnosti a sociálneho inžinierstva,
• e-learningové školenia a kurzy,
• informovanie o najnovších trendoch v oblasti KIB.

Skratka	Vysvetlenie
ŠU	štúdia uskutočniteľnosti
NKIVS	Národná koncepcia informatizácie verejnej správy
ÚPPVII/ SRIT	Úrad podpredsedu vlády SR pre investície a informatizáciu, Sekcia riadenia informatizácie
eGov (e-Gov)	e-Government
RZ	reformný zámer
MV SR	Ministerstvo vnútra Slovenskej republiky
SVS	Sekcia verejnej správy
OP EVS	Operačný program Efektívna verejná správa
ISVS	informačný systém verejnej správy
META IS	metainformačný systém
HK	hodnotiace kritérium
ÚPVS	Ústredný portál verejnej správy
SLA	Service Level Agreement
ŽoNFP, resp NFP	žiadosť o nenávratný finančný prostriedok, nenávratný finančný prostriedok