Príloha č. 8 Výzvy

Minimálne náležitosti manažérskych produktov – verejná správa

Pre splnenie **podmienky poskytnutia príspevku č. 2** Výzvy „**Podmienka splnenia kritérií pre výber projektov**“ (časť B. písm. c), e)) je žiadateľ **povinný** pri vypracovaní **projektového zámeru**, **prístupu k projektu** a **katalógu požiadaviek** (ďalej ako „**manažérske produkty**“) postupovať v súlade s touto prílohou č. 8 Výzvy, ktorá obsahuje minimálne náležitosti manažérskych produktov. Táto príloha č. 8 Výzvy zároveň v **časti 2. a 3.** obsahuje vymedzenie **rozsahu oprávnených podaktivít** platných pre danú Výzvu**.**

1. Žiadateľ je povinný vypracovať manažérske produkty v rozsahu uvedenom v **tabuľkách č. 1a, 1b a 1c nižšie** a zároveň v zmysle **Vyhlášky 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.**

V zmysle **podmienky poskytnutia príspevku č. 4 Výzvy** „Podmienka splnenia maximálnej a minimálnej výšky príspevku“ je:
Minimálna výška NFP: nad 200 000 EUR.
Maximálna výška NFP: 450 000 EUR.

Postup a vzory pre vypracovanie manažérskych produktov, vrátane „**Zoznamu rizík a závislostí**“ sú zverejnené aj na stránke: https://mirri.gov.sk/sekcie/informatizacia/riadenie-kvality-qa/.

Upozorňujeme, že pre posúdenie splnenia **podmienky poskytnutia príspevku č. 2 Výzvy** „Podmienka splnenia kritérií pre výber projektov“ a **podmienky poskytnutia príspevku č. 9 Výzvy** „Podmienka, že projekt je v súlade s Vyhláškou č. **401/2023 Z. z.** o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy“ **žiadateľ musí mať všetky manažérske produkty nahraté** v Centrálnom metainformačnom systéme verejnej správy SR.

Tabuľka č.1a - Zoznam povinných kapitol a príloh **projektového zámeru**:

Potrebné pre výzvu	
Manažérske zhrnutie	**Áno**
Motivácia a rozsah projektu	**Áno**
Zainteresované strany/Stakeholderi	**Áno**
Ciele projektu a merateľné ukazovatele	**Áno**
Návrh organizačného zabezpečenia projektu	**Áno**
Alternatívy	**Áno**
Opis obmedzení, predpokladov, tolerancií	**Áno**
Opis požadovaných výstupov	**Áno**
Náhľad architektúry	**Áno, v závislosti od technického riešenia (pokiaľ budú predmetom projektu aj technické opatrenia)**
Opis rozpočtu	**Áno**
Detailný popis nákladov a prínosov	**Áno**
Postup a spôsob nacenenia projektu	**Áno**
Harmonogram projektu	**Áno**
Zoznam rizík a závislostí	**Áno**

Tabuľka č.1b - Zoznam povinných kapitol a príloh **prístupu k projektu**:

Potrebné pre výzvu	
Opis navrhovaného riešenia	**Áno**

Architektúra riešenia projektu na úrovni biznis vrstvy	**Áno, v závislosti od technického riešenia (pokiaľ budú predmetom projektu aj technické opatrenia)**
Architektúra riešenia projektu na úrovni aplikačnej vrstvy	**Áno, v závislosti od technického riešenia (pokiaľ budú predmetom projektu aj technické opatrenia)**
Architektúra riešenia projektu na úrovni dátovej vrstvy	**Áno, v závislosti od technického riešenia (pokiaľ budú predmetom projektu aj technické opatrenia)**
Architektúra riešenia projektu na úrovni technologickej vrstvy	**Áno, v závislosti od technického riešenia (pokiaľ budú predmetom projektu aj technické opatrenia)**
Infraštruktúra navrhovaného riešenia	**Áno, v závislosti od technického riešenia (pokiaľ budú predmetom projektu aj technické opatrenia**
Bezpečnostná architektúra	**Áno, v závislosti od technického riešenia (pokiaľ budú predmetom projektu aj technické opatrenia)**
Špecifikácia údajov spracovaných v projekte, čistenie údajov	**Áno, v závislosti od technického riešenia (pokiaľ budú predmetom projektu aj technické opatrenia)**
Závislosti na ostatné IS/Projekty	**Áno**
Zdrojové kódy	**Áno, v závislosti od technického riešenia (pokiaľ budú predmetom projektu aj technické opatrenia)**
Prevádzka a údržba výstupov projektu	**Áno, v závislosti od technického riešenia (pokiaľ budú predmetom projektu aj technické opatrenia)**
Požiadavky na personál	**Áno, v závislosti od technického riešenia (pokiaľ budú predmetom projektu aj technické opatrenia)**
Implementácia a preberanie výstupov projektu	**Áno**

Tabuľka č.1c - Zoznam povinných kapitol a príloh v **Katalógu požiadaviek dokumente**:

Potrebné pre výzvu	
Katalóg požiadaviek	**Áno**

2. Rozsah povinných podaktivít platných pre danú Výzvu:

Žiadateľ je povinný v rámci projektového zámeru a ŽoNFP (časť 7. Popis projektu) deklarovať, že má ku dňu predloženia ŽoNFP zrealizované nasledovné aktivity:[1]

- vytvorenú stratégiu kybernetickej bezpečnosti,
- vytvorené bezpečnostné politiky kybernetickej bezpečnosti,
- vykonanú inventarizáciu aktív, klasifikáciu informácií a kategorizáciu sietí a informačných systémov,
- realizovanú analýzu rizík a analýzu dopadov spolu, vrátane riadenia rizík.

Ak žiadateľ nemá tieto aktivity zrealizované ku dňu predloženia ŽoNFP, je povinný ich realizovať v rámci projektu.

[1] V zmysle Vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení v znení vyhlášky č. 264/2023 Z. z.

3. Rozsah oprávnených podaktivít platných pre danú Výzvu:

Výzva je primárne určená pre tie oblasti, kde žiadateľ identifikuje najvyššiu mieru rizika a najvyššie dopady, prípadne kde má najvyššiu mieru nesúladu s legislatívnymi požiadavkami, vyplývajúce z vykonaného auditu kybernetickej bezpečnosti alebo samohodnotenia, prípadne z vykonanej analýzy rizík. Pri výbere a nastavení oprávnených podaktivít žiadateľ vychádza najmä z požiadaviek určených zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej ako „zákon o KB"), zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení zákona č. 301/2023 Z. z. a príslušných vykonávacích právnych predpisov.

Predmetom projektu môže byť aj financovanie nákladov spojených s auditom kybernetickej bezpečnosti podľa § 29 zákona č. 69/2018 Z. z. **zrealizovaným v čase od vyhlásenia výzvy do jej ukončenia.**
Zároveň je možné pre-financovať aj pravidelne sa opakujúce a legislatívou vyžadované činnosti, ako je napr. každoročná aktualizácia analýzy rizík, inventarizácia aktív, klasifikácia informácií a kategorizáciu sietí a IS a pod.

Pri týchto činnostiach je potrebné v projektovom zámere/ŽoNFP preukázať, že nejde o preplatenie aktivít z minulosti, ale ide o novú aktivitu realizovanú v čase platnosti tejto Výzvy, a že ide skutočne napr. o pravidelnú aktualizáciu.

Upozorňujeme:
Súčasťou oprávnených aktivít v oblasti vzdelávania je zaškolenie na implementovanú technológiu. **Podpora sa netýka školení pre zamestnancov za účelom zvýšenia ich povedomia v oblasti kybernetickej bezpečnosti**.

Jednotlivé podaktivity žiadateľ popíše aj v ŽoNFP v časti 7. Popis projektu, prípadne uvedie v ŽoNFP (časť 7. Popis projektu) odkaz na konkrétnu časť Projektového zámeru, kde sú dané podaktivity popísané.

Názov podaktivity		Bližšie činnosti
a)	Organizácia kybernetickej a informačnej bezpečnosti	- Vypracovanie alebo aktualizácia bezpečnostnej dokumentácie vrátane rozsahu a spôsobu plnenia všeobecných bezpečnostných opatrení; - ~~zabezpečenie outsourcingu role manažéra kybernetickej bezpečnosti v súlade so zákonom o KB od externého subjektu;~~ - vypracovanie a implementácia špecifických interných riadiacich aktov pre vybrané oblasti kybernetickej a informačnej bezpečnosti; - vypracovanie štatútu bezpečnostného výboru; - vypracovanie bezpečnostného projektu informačného systému verejnej správy.[2]
b)	Riadenie rizík	- Identifikácia všetkých aktív súvisiacich so zariadeniami na spracovanie informácií a centrálne zaznamenávanie inventáru týchto aktív podľa ich hodnoty vrátane určenia ich vlastníka, ktorý definuje požiadavky na ich dôvernosť, dostupnosť a integritu; - implementáciu systému pre inventarizáciu aktív; - riadenie rizík pozostávajúce z identifikácie zraniteľností, identifikácie hrozieb, identifikácie a analýzy rizík s ohľadom na aktívum, určenie vlastníka rizika, implementácie organizačných a technických bezpečnostných opatrení, analýzy funkčného dopadu a pravidelného preskúmavania identifikovaných rizík v závislosti od aktualizácie prijatých bezpečnostných opatrení; - vypracovanie a implementácia interného riadiaceho aktu riadenia rizík kybernetickej a informačnej bezpečnosti.
c)	Personálna bezpečnosť	- Vypracovanie postupov pri zaradení osoby do niektorých z bezpečnostných rolí, zavedenie plánu rozvoja bezpečnostného povedomia a vzdelávania, vypracovanie spôsobov hodnotenia účinnosti plánu rozvoja bezpečnostného povedomia, určenie pravidiel a postupov na riešenie prípadov porušenia bezpečnostnej politiky, zavedenie postupov pri skončení

[2] Príloha č. 3 k vyhláške č. 179/2020 Z. z. Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu z 22. júna 2020, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

Formátované: Medzera Za: 6 b

Formátované: Písmo: Tučné

		pracovnoprávneho vzťahu alebo iného obdobného vzťahu, zavedenie postupov pri porušení bezpečnostných politík; - vypracovanie alebo aktualizácia interného riadiaceho aktu s bezpečnostnými zásadami pre koncových používateľov; - vypracovanie a implementácia postupov a procesov upravujúcich personálnu bezpečnosť organizácie prostredníctvom interného riadiaceho aktu.
d)	Riadenie prístupov	- Vypracovanie a implementácia zásad riadenia prístupov osôb k sieti a informačnému systému; - zavedenie, implementácia alebo aktualizácia centrálneho nástroja na správu a overovanie identity, nástroja na riadenie prístupových oprávnení vrátane privilegovaných prístupových práv a kontroly prístupových účtov a prístupových oprávnení; - vypracovanie a implementácia postupov a procesov upravujúcich riadenie prístupov organizácie.
e)	Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami	- Vypracovanie analýzy rizík tretích strán a celého dodávateľského reťazca, vrátane analýzy politických rizík; - analýza a posúdenie súladu všetkých aktuálnych zmlúv s tretími stranami so zákonom o KB a dobrou praxou; - vypracovanie návrhov dodatkov zmlúv s treťou stranou spolu s návrhom potrebných úprav na zabezpečenie súladu so zákonom KB; - vypracovanie a implementácia interného riadiaceho aktu upravujúceho zásady kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami.
f)	Bezpečnosť pri prevádzke informačných systémov a sietí	- Zavedenie opatrení a interného riadiaceho aktu v oblasti riadenia zmien, riadenia kapacít, inštalácie softvéru v sieťach a informačných systémoch, inštalácia zariadení v sieťach a informačných systémoch, zaznamenávanie bezpečnostných záznamov a zaznamenávanie a vyhodnocovanie prevádzkových záznamov; - implementácia technických riešení podporujúcich riadenie bezpečnosti pri prevádzke, napr. nástroj pre riadenie, evidenciu a schvaľovanie zmien, evidenciu bezpečnostných incidentov, konfiguračný manažment bezpečnostných nastavení; - obstaranie služieb pre potreby správy prevádzkovej zálohy, kópie archivačnej zálohy a kópie inštalačných médií, vrátane určenia spôsobu ich ukladania, testov funkcionality dátových nosičov, testov obnovy, fyzického uloženia druhej kópie archivačnej zálohy v inom objekte a minimalizovania rizika poškodenia alebo zničenia dátových nosičov archivačných záloh vplyvom prírodných živlov alebo havárie.
g)	Hodnotenie zraniteľností a bezpečnostné aktualizácie	- Zavedenie, implementácia alebo aktualizácia nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí a detegovanie existujúcich zraniteľností technických prostriedkov a ich častí, prípadne obstaranie tejto funkcionality ako externej služby; - vypracovanie a implementácia interného riadiaceho aktu upravujúceho proces riadenia implementácie bezpečnostných aktualizácií a záplat; - implementácia nástroja na centrálne riadenie a aplikovanie bezpečnostných záplat a pod.
h)	Ochrana proti škodlivému kódu	- Vypracovanie interného riadiaceho aktu s požiadavkami na určenie zodpovednosti používateľov, pravidiel pre inštaláciu a monitorovania potenciálnych ciest prieniku škodlivého kódu; - implementácia alebo aktualizácia nástrojov na ochranu, ktoré okrem iného vykonávajú kontrolu prístupu k digitálnemu obsahu, pravidelné kontroly úložísk vrátane cloudových riešení, zabraňujú prístupu neoprávnených používateľov filtrovaním obsahu a zamedzením odinštalovať alebo zakázať funkcie systému na ochranu proti škodlivému kódu;

		- vypracovanie a implementácia pravidiel súvisiace s ochranou proti škodlivému kódu; - implementácia centralizovaného systému riešenia ochrany pred škodlivým kódom s pravidelným monitorovaním vrátane detekcie inštalácie nelegálneho obsahu alebo škodlivého softvéru prostredníctvom automatizovaných nástrojov.
i)	Sieťová a komunikačná bezpečnosť	- Implementácia nástrojov na ochranu integrity sietí, ktoré zabezpečujú riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami, implementácia segmentácie sietí, implementácia alebo obnova firewall-u, revízia firewall pravidiel; - zavedenie bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a vzdialený prístup, napríklad implementáciou dvojfaktorovej autentizácie alebo kryptografických prostriedkov; - vytvorenie alebo aktualizácia dokumentácie počítačovej siete, ktorá obsahuje evidenciu všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológiu siete a využitie IP rozsahov; - realizácia/aktualizácia segmentácie sietí v súlade s pravidlami klasifikácie a kategorizácie; - vypracovanie a implementácia interného riadiaceho aktu upravujúceho pravidlá sieťovej a komunikačnej bezpečnosti; - implementácia automatizovaného nástroja na identifikáciu neoprávnených sieťových spojení na hranici s vonkajšou sieťou, na blokovanie neoprávnených spojení, na monitorovanie bezpečnosti, na detekciu prienikov a prevenciu prienikov identifikáciou nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky a ďalších povinností alebo vo forme funkcionalít, prípadne licencií iných už existujúcich nástrojov; - implementácia sond detekcie a prevencie prieniku, najmä na serveroch podporujúcich základné služby informačných technológií verejnej správy.
j)	Akvizícia, vývoj a údržba informačných technológií verejnej správy	- Implementácia ochrany informácií v transakciách informačných technológií verejnej správy, a to najmä implementáciou elektronického podpisu a elektronickej pečate na kvalifikovanej úrovni bezpečnosti certifikátov, šifrovanie komunikačných kanálov a zabezpečenie komunikačných protokolov; - vykonanie bezpečnostného testovania pri všetkých vydaniach alebo verziách počas vývojového cyklu kritických informačných technológií verejnej správy; - zavedenie pravidiel a postupov definujúcich požiadavky na akvizíciu, vývoj a údržbu sietí a informačných systémov, ktoré sa uplatňujú na obstarávané, vyvíjané a udržiavané komponenty s digitálnymi prvkami (napríklad prostredníctvom interného riadiaceho aktu); - vypracovanie metodiky softvérového vývoja v podobe interného riadiaceho aktu, definujúce bezpečnostné požiadavky na všetky fázy životného cyklu vývoja SW (SSDLC).
k)	Zaznamenávanie udalostí a monitorovanie	- Implementácia centrálneho Log manažment systému pre zber a ukladanie logov z jednotlivých informačných systémov; - implementácia centrálneho nástroja na zaznamenávanie činností sietí a informačných systémov a používateľov a identifikovanie bezpečnostných incidentov (SIEM); - vypracovanie dokumentácie spôsobu monitorovania a fungovania Log manažment systému a centrálneho nástroja na bezpečnostné monitorovanie a zadefinovanie spôsobu evidencie prevádzkových záznamov, ich vyhodnocovania, spôsobu hlásenia podozrivej aktivity, zodpovednej osoby a ďalších povinností;

		- špecifikácia všetkých udalostí, ktoré musia byť zaznamenávané a konfigurácia prvkov informačných technológií verejnej správy, vrátane dokumentácie rozsahu dát zaznamenávaných log súborov; - vypracovanie interného riadiaceho aktu, ktorý obsahuje a upravuje povinnosti definované platnou legislatívou; - obstaranie služby kontroly záznamov (SOC as a service) na dennej báze, vrátane podpory analýzy bezpečnostne relevantných udalostí a vykonávanie bezpečnostného dohľadu napr. v režime 24/7; - implementácia automatizovaných systémov vykonávajúcich dohľad pred neoprávnenými zásahmi, neautorizovaným prístupom, najmä pred zmenami a zničením, vrátane monitorovania kapacity systémov a návrh adekvátnych opatrení na ukladanie záznamov a systému logovania.
l)	Riešenie kybernetických bezpečnostných incidentov	- Vypracovanie štandardov a postupov riešenia kybernetických bezpečnostných incidentov, vrátane definovania zodpovedností zamestnancov a ďalších povinností; - obstaranie služby monitorovania a analyzovania udalostí v sieťach a informačných systémoch vrátane detekcie, zberu relevantných informácií, vyhodnocovania a riešenia zistených kybernetických bezpečnostných incidentoch a vykonávania napr. forenzných analýz v snahe minimalizovať výskyt a dopad kybernetických bezpečnostných incidentov; - implementácia nástroja na detekciu, nástroja na zber a nepretržité vyhodnocovanie a evidenciu kybernetických bezpečnostných udalostí; - vypracovanie interného riadiaceho aktu obsahujúceho a upravujúceho povinnosti týkajúce sa riešenia kybernetických bezpečnostných incidentov; - vypracovanie plánov a spôsobov riešenia kybernetických bezpečnostných incidentov.
m)	Kryptografické opatrenia	- Implementácia opatrení za účelom zabezpečenia autenticity a integrity súborov; - implementácia kryptografických opatrení nad zálohami systémov a dát; - vypracovanie a implementácia interného riadiaceho aktu upravujúceho používanie kryptografických prostriedkov a šifrovania; - definovanie pravidiel využitia kryptografických prostriedkov používajúcich dostatočne odolné kryptografické mechanizmy na ochranu údajov pri ich prenose alebo uložení v rámci sietí a informačných systémov; - vypracovanie a dokumentácia systému správy kryptografických kľúčov a certifikátov; - implementácia systému správy kryptografických kľúčov a certifikátov a pod.
n)	Kontinuita prevádzky	- Vypracovanie stratégie a krízových plánov prevádzky na základe analýzy vplyvov kybernetického bezpečnostného incidentu na základnú službu; - vypracovanie plánov kontinuity prevádzky a ich prvotné otestovanie v reálnom prostredí organizácie a zapracovanie nedostatkov z výsledkov testovania; - vypracovanie interného riadiaceho aktu obsahujúceho a upravujúceho kontinuitu prevádzky následkom kybernetického bezpečnostného incidentu alebo inej krízovej situácie; - vypracovanie postupov zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu alebo inej krízovej situácie; - implementácia systému zálohovania.
o)	Audit a kontrolné činnosti	- Vypracovanie programu posúdenia bezpečnosti na definované informačné technológie verejnej správy, hodnotenia zraniteľností a penetračných testov; - obstaranie prvého alebo opakovaného auditu kybernetickej bezpečnosti v súlade so zákonom o KB; - obstaranie externých testov zraniteľností, penetračných testov a pod.
