projekt_2800_Projektovy_zamer_detailny

PROJEKTOVÝ ZÁMER

podľa vyhlášky MIRRI č. 401/2023 Z. z.

Povinná osoba	Regionálny úrad verejného zdravotníctva so sídlom v Trnave
Názov projektu	Kybernetická a informačná bezpečnosť RÚVZ v Trnave
Zodpovedná osoba za projekt	Mgr. Tomáš Hauko, MPH
Realizátor projektu	Regionálny úrad verejného zdravotníctva so sídlom v Trnave
Vlastník projektu	Mgr. Tomáš Hauko, MPH

Schvaľovanie dokumentu

Položka	Meno a priezvisko	Organizácia	Pracovná pozícia	Dátum	Podpis (alebo elektronický súhlas)
Vypracoval	Denis Dojčan	RÚVZ so sídlom v Trnave	Manažér kybernetickej bezpečnosti	19.06.2024	
Schválil	Mgr. Tomáš Hauko, MPH	RÚVZ so sídlom v Trnave	Regionálny hygienik a generálny tajomník služobného úradu	02.07.2024	

1. HISTÓRIA DOKUMENTU

Verzia	Dátum	Zmeny	Meno
0.01	19.06.2024	prvá verzia dokumentu	Denis Dojčan
0.02	21.06.2024	druha verzia dokumentu	Denis Dojčan
1.00	01.07.2024	zapracovanie pripomienok a súladu s vyhláškou č. 401/2023 Z. z., finálna verzia v súlade so ŽoNFP	Denis Dojčan

2. ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE

V súlade s **Vyhláškou** MIRRI SR **č. 401/2023 Z. z. o riadení projektov a zmenových požiadaviek v prevádzke IT VS** - je dokument "*Projektový zámer*" je určený na rozpracovanie informácií k projektu z pohľadu aktuálneho stavu, aby bolo možné rozhodnúť o pokračovaní prípravy projektu, alokovaní rozpočtu, ľudských zdrojov a po prechode do iniciačnej fázy aj z pohľadu budúceho stavu a navrhovaného riešenia.

Dokument "*Projektový zámer*" je vypracovaný za účelom predloženia projektu s názvom "*Kybernetická a informačná bezpečnosť RÚVZ v Trnave* " v rámci Výzvy č. OPII-PSK-MIRRI-611-2024-DV-EFRR na predkladanie Žiadostí o poskytnutie NFP "***Podpora v oblasti KIB na regionálnej úrovni – VS***".

Projektový zámer obsahuje povinné kapitoly v súlade s prílohou č. 8 Výzvy Minimálne náležitosti manažérskych produktov – verejná správa: Manažérske zhrnutie, Motivácia a rozsah projektu, Zainteresované strany/Stakeholderi, Ciele projektu a merateľné ukazovatele, Návrh organizačného zabezpečenia projektu, Alternatívy, Opis obmedzení, predpokladov, tolerancií, Opis požadovaných výstupov, Náhľad architektúry, Opis rozpočtu, Detailný popis nákladov a prínosov, Postup a spôsob nacenenia projektu, Harmonogram projektu, Zoznam rizík a závislostí

Projekt umožňuje realizovať opatrenia KIB definované najmä v zákonoch č. 69/2018 Z. z. o KB a o zmene a doplnení niektorých zákonov (ďalej len „*zákon č. 69/2018 Z. z.*") a č. 95/2019 Z. z. o IT vo VS a o zmene a doplnení niektorých zákonov (ďalej len „*zákon o ITVS*").

Hlavnou motiváciou je realizácia kyberbezpečnostných opatrení definovaných v Z.z. 69/2018 a v zákone o ISVS.

Primárne ide o tie opatrenia, ktoré vykazujú najväčší nesúlad s uvedenými právnymi normami a vyhláškou 362/2018 Z. z.. Vďaka realizácii týchto opatrení budú IS RÚVZ so sídlom v Trnave chránené v maximálnej možnej miere pred kybernetickým incidentom, ktorý by mohol mať na poskytovanie služieb a prevádzku IS RÚVZ so sídlom v Trnave **nasledovný dopad**:

- zamedzenie kontinuity základnej služby – MIS registratúra,
- zamedzenie výkonu ochrany verejného zdravotníctva u občanov v Trnavskom kraji,
- porušenie dôvernosti a integrity osobných údajov, dôverných a interných informácií a porušenie lekárskeho tajomstva
- zamedzenie výkonu kontroly štátneho dozoru a tým aj dohľad nad povinnými opatreniami v jednotlivých subjektov v Trnavskom kraji.

Projekt je formulovaný tak, aby po jeho realizácii nastal čo najväčší súlad zabezpečenia KIB so zákonom o KB a so zákonom o ISVS.

- **Obmedzenia projektu**

Z hľadiska technického, personálneho, odborného, ale ani legislatívneho RÚVZ so sídlom v Trnave neeviduje žiadne obmedzenia, ktoré by mohli ovplyvniť úspešnú realizáciu projektu.

- **Predpoklady projektu**

Pri zvyšovaní úrovne KB a splnenie Z. z. 69/2018 a Vyhlášky Národného bezpečnostného úradu č. 362/2018 v infraštruktúre RÚVZ Trnava sa predpokladá výpadok do maximálne nepretržitých 10 hodín na každej pobočke a 4 hodiny s prestávkami počas výmeny zariadení na sieti.

- **Tolerancie projektu**

Možný výpadok základnej služby – MIS registratúry je možný maximálne na 48 hodín na každej pobočke. Predpokladaná odstávka bude práve pri implementácií segmentácie infraštruktúry siete organizácie a pri nasadzovaní „firewallu“ a „switch-ov“ obstarávaných z projektu.

2.1 Použité skratky a pojmy

ID	skratka	popis
1	KIB	kybernetická a informačná bezpečnosť
2	MIRRI	Ministerstvo investícií, regionálneho rozvoja a informatizácie SR
3	SR	Slovenská republika
4	IT	informačné technológie
5	VS	verejná správa
6	NFP	nenávratný finančný príspevok
7	KB	kybernetická bezpečnosť
8	ITVS	informačné technológie verejnej správy
9	OPII	Operačný program Integrovaná infraštruktúra
10	EFRR	Európsky fond regionálneho rozvoja
11	IB	informačná bezpečnosť
12	TT	Trnava
13	RÚVZ	Regionálny úrad verejného zdravotníctva so sídlom v Trnave
14	PN	Piešťany
15	HC	Hlohovec
16	TTSK	Trnavský samosprávny kraj
17	MZ	Ministerstvo zdravotníctva SR
18	NR SR	Národnej rady SR
19	ISVS	informačných systémov verejnej správy

20	MU	merateľné ukazovatele
21	MJ	merná jednotka
22	NBÚ	Národný bezpečnostný úrad
23	IKT	informačno-komunikačné technológie
24	NKIVS	Národná koncepcia informatizácie verejnej správy
25	HW	hardvér
26	SW	softvér
27	RV	Riadiaci výbor
28	MJ	merná jednotka
29	JC	jednotková cena
30	NFP	nenávratný finančný príspevok
31	VO	verejné obstarávanie
32	HK	hodnotiace kritérium
33	KPI	výkonnostný ukazovateľ
34	ŽoNFP	Žiadosť o nenávratný finančný príspevok
35	MIS	Administratívny systém úradu, ktorý podporuje IS VS - registratúra
36	TŠ	Technická špecifikácia (dokument, popisujúci kontext pre technické začlenenie riešenia do prostredia organizácie, s jeho technickými, integračnými, architektúrnymi a bezpečnostnými požiadavkami)
37	WF	Workflow = pracovný proces, zobrazený postupnosťou úkonov
38		

2.2 Konvencie pre typy požiadaviek (príklady)

Hlavné kategórie požiadaviek v zmysle katalógu požiadaviek, rozdeľujeme na funkčné, nefunkčné a technické. V rámci projektu budú definované tri základné typy požiadaviek:

Funkcionálne (používateľské) požiadavky majú nasledovnú konvenciu:

FRxx

- U – užívateľská požiadavka
- R – označenie požiadavky
- xx – číslo požiadavky

Nefunkčné (kvalitatívne, výkonové - Non Functional Requirements - NFR) požiadavky majú nasledovnú konvenciu:

NRxx

- N – nefukčná požiadavka (NFR)
- R – označenie požiadavky
- xx – číslo požiadavky

Tabuľka 1 Hlavné kategórie požiadaviek v zmysle katalógu požiadaviek

ID	SKRATKA	POPIS
1.	U	Užívateľská požiadavka

2.	P	Procesná požiadavka
3.	R	Požiadavka na reporting
4.	I	Integračná požiadavka
5.	C	Kapacitné požiadavky procesov
6.	S	Požiadavka na bezpečnosť
7.	O	Prevádzková požiadavka (Operations)
8.	D	Požiadavka na dokumentáciu
9.	L	Legislatívna požiadavka
10.	O	Ostatné
11.	...	...

3. DEFINOVANIE PROJEKTU

3.1 Manažérske zhrnutie

Opis východiskovej situácie

Projekt s **názvom** „*Kybernetická a informačná bezpečnosť RÚVZ v Trnave*“ (ďalej len „*projekt*“) bol vypracovaný s **hlavným cieľom** “*zlepšovanie technologického, procesného, infraštruktúrneho, vedomostného a organizačného zabezpečenia zručností a kapacít pre plnenie úloh v oblasti KIB v prostredí orgánov štátnej a VS*” a zabezpečiť súlad s legislatívnymi požiadavkami v oblasti KIB a umožniť realizovať a financovať opatrenia KIB definované najmä v zákonoch č. 69/2018 Z. z. a č. 95/2019 Z. z., najmä v týchto oblastiach:

- riadenie rizík KIB,
- personálna bezpečnosť,
- riadenie prístupov,
- bezpečnosť pri prevádzke IS a sietí,
- ochrana proti škodlivému kódu,
- sieťová a komunikačná bezpečnosť,
- zaznamenávanie udalostí a monitorovanie,
- riešenie kybernetických bezpečnostných incidentov,
- kontinuita prevádzky,
- audit, riadenie súladu a kontrolné činností.

Predmetom projektu je zvýšenie informačnej a kybernetickej bezpečnosti, čo podporí integritu a dôvernosť spracúvaných údajov a zároveň splnenie požiadaviek Z. z. 69/2018 a Vyhlášky Národného bezpečnostného úradu č. 362/2018. Údaje aktuálne pri kyberbezpečnostnom incidente sú vystavené riziku úniku prípadne zmeny integrity a požadované opatrenia pokryté z projektu zvýšia úroveň kyberbezpečnosti a možnému útočníkovi znemožnia rôzne druhy infiltrácie do infraštruktúry organizácie a zamedzia možných rozsah škôd či prístup k údajom, ktoré by mohol možný útočník ovplyvniť.

RÚVZ so sídlom v Trnave chce hlavný cieľ dosiahnuť s pomocou finančných prostriedkov z dopytovo-orientovanej výzvy č. OPII-PSK-MIRRI-611-2024-DV-EFRR, “*Podpora v oblasti KIB na regionálnej úrovni – VS*” (ďalej len „*Výzva*“):

Tabuľka 2 Príslušnosť projektu k priorite

názov	**popis**

Príslušnosť dopytového projektu programu: Program Slovensko 2021 – 2027	Predkladaný dokument je manažérskym produktom v zmysle Vyhlášky Úradu podpredsedu vlády SR pre investície a informatizáciu č. 401/2023 Z. z. o riadení projektov **Program Slovensko 2021 – 2027** **Priorita:** 1P1 Veda, výskum a inovácie. **Špecifický cieľ:** RSO 1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy Projekt prispieva k výsledkom Partnerskej dohody **Opatrenie:** 1.2.1 Podpora v oblasti informatizácie a digitálnej transformácie (Oblasť - Kybernetická a informačná bezpečnosť)
Indikatívna výška finančných prostriedkov určených na realizáciu projektu:	309 431,16 €
Časový horizont projektu:	09/2024 - 12/2025

Po implementácii projektu bude RÚVZ so sídlom v Trnave pripravené efektívnejšie riadiť KIB vo svojej oblasti a čeliť interným a externým hrozbám v oblasti KIB.

Výsledky Samohodnotenia zo dňa 20.12.2023

RÚVZ so sídlom v Trnave má vykonané **Samohodnotenia zo dňa 20.12.2023** (ďalej len „*samohodnotenie*“), v rámci ktorého:

Správa aktív: Má identifikované informačné aktíva a určenú ich klasifikáciu pre dôveryhodnosť, integritu a dostupnosť; všetky podporné aktíva; všetkých dodávateľov, ktorí svojím poskytovaním služieb podporujú prevádzku ZS; vlastníkov ku všetkým identifikovaným aktívam; eviduje všetky aktíva podieľajúcich sa na prevádzke ZS. Proces na aktualizáciu evidencie sa vedie len čiastočne.

Manažment konfigurácií: V rámci manažmentu konfigurácie sa čiastočne vedie evidencia o konfiguračných nastaveniach identifikovaných aktív a služieb a nie je zavedený proces pravidelného aktualizovania záznamov v evidencii konfigurácií aktív a služieb.

Technické zraniteľnosti: V rámci tejto oblasti získava informácie o známych zraniteľnostiach od dodávateľov aktív, SK-CERT, CSIRT-SK, a pod., pričom len čiastočne vyhodnocuje dopad známych zraniteľností na aktíva a vyhodnocuje riziko spojené s týmito zraniteľnosťami.

Prevádzkový monitoring: Čiastočne má určené, pre ktoré aktíva a komponenty v prostredí potrebuje mať nastavený prevádzkový monitoring a takisto vykonáva čiastočný monitoring týchto parametrov tak, aby mal nepretržitý prehľad o prostredí.

Bezpečnostný monitoring: Nemá implementovaný nástroj na výkon bezpečnostného monitoringu nad aktívami, ktoré sa podieľajú na základnej službe a má nastavený proces, ktorým vie reagovať na kybernetický bezpečnostný incident.

Personálna bezpečnosť: Čiastočne vykonáva kontrolu dodržiavania bezpečnostných politík zo strany vlastných zamestnancov a zamestnancov dodávateľov.

Riadenie rizík: neidentifikuje a nevyhodnocuje riziká kybernetickej bezpečnosti, pričom čiastočne navrhuje a implementuje bezpečnostné opatrenia kybernetickej bezpečnosti, ktorými znižuje neakceptovateľne veľké zvyškové riziká.

Riadenie bezpečnosti sietí: nemá implementovanú bezpečnostnú sieťovú segmentáciu a ani nevykonáva aktívnu a priebežnú správu pravidiel na zariadeniach oddeľujúcich jednotlivé sieťové segmenty.

Riadenie prístupov: má zadefinované rozsahy logických a aj fyzických prístupových oprávnení vlastných zamestnancov a zamestnancov dodávateľov k všetkým svojim aktívam a vykonáva pravidelnú kontrolu nad nastavenými rozsahmi prístupových oprávnení na aktívach.

Riadenie procesov pre správu a údržbu IS: nemá zavedený proces zmenového konania (Change management) a proces incident manažmentu, má zavedený proces zálohovania a proces kontinuity procesov a služieb a obnovu po havárii.

Riadenie dodávateľských vzťahov: čiastočne monitoruje na pravidelnej báze parametre služieb, ktoré poskytujú dodávatelia.

Riadenie IB a KB

Riešenie plnenia povinností vyplývajúcich zo zákona o KB bezpečnosti zabezpečuje Útvar regionálneho hygienika a generálneho tajomníka služobného úradu, pod ktorý okrem iného spadá i činnosť manažéra KB.

Za KB zodpovedajú:

- Generálny tajomník služobného úradu,
- Manažér KB,
- Správca IT,
- Všetky oprávnené osoby v rozsahu svojich pracovných kompetencií, ktoré im vyplývajú z ich pracovnej náplne.

Pre všetky oprávnené osoby, vrátane správcu IT a manažéra KB sú záväzné bezpečnostné smernice RÚVZ so sídlom v Trnave.

Manažment kybernetických bezpečnostných incidentov vykonáva manažér KB v súčinnosti so správcom IT, v prípade závažných kybernetických bezpečnostných incidentov s generálnym tajomníkom služobného úradu.

Manažér KB zabezpečuje plnenie povinností a požiadaviek na KB z pohľadu zákona. Zároveň nahlasuje bezpečnostné incidenty na NBÚ a tvorí smernice s dokumentáciu v oblasti IKT a KB. Z jeho pozície vyplýva i možnosť predkladať návrhy a oznamovať informácie v oblasti KB priamo štatutárnemu orgánu a jeho nezávislosť od riadenia prevádzky a vývoja služieb IT. Riadenie je priamo zahrnuté v smernici „*SMERNICA SM60 – KYBERNETICKÁ BEZPEČNOSŤ*“ zo dňa 01.12.2021.

Bezpečnostná dokumentácia

RÚVZ so sídlom v Trnave TT má prijatú nasledovnú bezpečnostnú dokumentáciu vypracovanú podľa zákona č. 69/2018 Z. z. a zákona o ITVS:

* SMERNICA SM60 – KYBERNETICKÁ BEZPEČNOSŤ zo dňa 01.12.2021, ktorá zahŕňa bezpečnostné smernice:

S01 Organizácia informačnej bezpečnosti

S02 Prevádzka automatizovaných IS

S03 Bezpečnosť sietí a IS

S04 Objektová bezpečnosť

S05 Riadenie kybernetickej bezpečnosti

S06 Tretie strany - dodávatelia

S07 Postupy pri obnove kontinuity prevádzky základnej služby

a odstraňovanie následkov kybernetického bezpečnostného incidentu

* SMERNICA SM23 – SMERNICA PRE POUŽÍVANIE INTERNETU (okrem elektronickej pošty) zo dňa 01.07.2022

* SMERNICA SM54 - SMERNICA PRE POUŽÍVANIE, ÚSCHOVU A OCHRANU EXTERNÝCH DISKOV, USB KĽÚČOV, CD a DVD zo dňa 01.07.2022

* SMERNICA SM71 Stratégia informačnej a kybernetickej bezpečnosti zo dňa 01.09.2023.

Má aktualizované SLA dohody a zmluvy s tretími stranami, týkajúce sa kybernetickej bezpečnosti a notifikačnej povinnosti u dodávateľov, ktorí sa podieľajú na prevádzke kritických informačných systémov organizácie. V rámci SLA dohody je aj zoznam zamestnancov, ktorí sa priamo podieľajú na prevádzke kritických informačných systémov organizácie. Uvedená dokumentácia je základným prvkom riadenia KIB RÚVZ so sídlom v Trnave. Z tejto dokumentácie zároveň vyplýva potreba zavedenia ďalších opatrení pre riadenie KIB s dôrazom na oddelenie riadiacej, výkonnej a kontrolnej funkcie. V rámci stratégie informačnej a kybernetickej bezpečnosti vyplývajú povinnosti, ako pre IT oddelenie a manažéra kybernetickej bezpečnosti, tak aj bezpečnosť zamestnancov a postupy práce pri spracúvaní osobných údajov, dôverných a interných informácií. Stratégia informačnej a kybernetickej bezpečnosti ďalej rieši personálne postupy, revízie zoznamu prístupov interných zamestnancov a tretích strán, či postupy pri obnove prevádzky, v prípade výpadku alebo postupy na testovanie výpadkov, či integrity záloh, v prípade straty dát spoločne s postupmi na nakladanie so zálohami a ich následne ukladanie a udržiavanie integrity, či dôvernosti.

Výstupy a výsledky tohto projektu budú zároveň plniť ciele definované v “*Stratégii informačnej a kybernetickej bezpečnosti*” a požiadavky interných riadiacich smerníc v oblasti IB a KB a ostatných relevantných dokumentov RÚVZ so sídlom v Trnave.

Základné informácie o projekte

Projekt je možné rozdeliť na 2 časti:

- nákup a implementácia HW a SW,
- organizačné a technické opatrenia za účelom zabezpečenia súladu so zákonom o KB.

Zároveň pôjde o:

1 – vykonanie auditu kybernetickej bezpečnosti

2 – vytvorenie bezpečnostnej politiky KB,

3 – vykonanú inventarizáciu aktív, klasifikáciu informácií a kategorizáciu sietí a IS,

4 - realizovanú analýzu rizík a analýzu dopadov spolu, vrátane riadenia rizík.

Cieľová skupina

Aj keď je cieľová skupina v predmetnej výzve nerelevantná, cieľovú skupinu definujeme ako beneficientov projektových výstupov. Cieľovou skupinu projektu je RUVZ SK, RÚVZ so sídlom v Trnave, interní zamestnanci RÚVZ so sídlom v Trnave, externí zamestnanci RÚVZ so sídlom v Trnave

MU

Tabuľka 3 MU projektu

kód MÚ projektu	názov MÚ	cieľová hodnota
PO095 / PSKPSOI12	Verejné inštitúcie podporované v rozvoji kybernetických služieb, produktov a procesov	1
PR017 / PSKPRCR11	Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov	1

Miesto realizácie projektu

- RÚVZ so sídlom v Trnave, Ulica Limbová 6053/6, 917 02 Trnava
- RÚVZ so sídlom v Trnave, Halenárska 23, 917 09 Trnava

Predpokladaný rozpočet

Predpokladaný rozpočet projektu (celkový objem NFP), ktorý má byť použitý na realizáciu projektu je 309 431,16 €. Bližšie údaje o finančnom rozdelení pre jednotlivé aktivity projektu sa nachádzajú v podkapitole 7. 1. ROZPOČET A PRÍNOSY

Sumarizácia hlavných parametrov hodnotenia projektu

Tabuľka 4 Sumarizácia hlavných parametrov hodnotenia projektu

ID	názov HK	parametre v projekte	zdroj
1	Miera rizík ohrozujúcich úspešnú realizáciu projektu	V rámci projektu bolo identifikovaných menej ako 10 % rizík z celkového počtu identifikovaných rizík v ŽoNFP s vysokou závažnosťou, ktoré ohrozujú úspešnú realizáciu projektu.	Príloha č. 1_REGISTER_RIZIK-a-ZAVISLOSTI_RUVZ TT_V2.xlsx
2	Administratívne, odborné a prevádzkové kapacity žiadateľa	RÚVZ so sídlom v Trnave disponuje (v súlade s podmienkami Výzvy) s dostatočnými odbornými kapacitami s náležitou odbornou spôsobilosťou a know-how na riadenie a implementáciu projektu v danej oblasti. Návrh organizačného zabezpečenia projektu je reálny a v súlade s podmienkami Výzvy.	Podkapitola 9 Projektový tím
3	Miera oprávnenosti výdavkov projektu	Všetky oprávnené aktivity vychádzajú z Výzvy PSK-MIRRI-611-2024-DV-EFRR	Akceptačné protokoly Monitorovacie správy k projektu
4	Dôležitosť KB u žiadateľa a potencionálny dopad kybernetických incidentov	Projekt implementuje nástroje do celej siete.	Interné smernice Akceptačné protokoly Protokoly testovania

3.2 Motivácia a rozsah projektu

ÚVZ so sídlom v Trnave - https://www.uvzsr.sk/web/ruvztt - je podľa zákona NR SR č. 355/2007 Z. z. o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov orgánom verejného zdravotníctva s územnou pôsobnosťou pre územný obvod okresov TT, PN a HC – TTSK kraj. Ako orgán verejného zdravotníctva v krajskom sídle odborne a metodicky vedie a koordinuje činnosť regionálnych úradov verejného zdravotníctva v TTSK a zabezpečuje pre ne laboratórne činnosti a diagnostiku. Je rozpočtová organizácia štátu zapojená finančnými vzťahmi na rozpočet MZ SR. Pri svojej činnosti postupuje podľa ustanovení zákona č. 355/2007 Z. z. a jeho vykonávacích predpisov, vrátane predpisov vydaných podľa zákona NR SR č. 19/2002 Z. z., ktorým sa ustanovujú podmienky vydávania aproximačných nariadení vlády SR v znení neskorších predpisov a taktiež podľa niektorých ďalších platných právnych predpisov dotýkajúcich sa problematiky ochrany verejného zdravia.

Poslaním je udržiavanie zdravých podmienok pre život TT regiónu prostredníctvom ovplyvňovania životného štýlu obyvateľov, výživových faktorov, prevenciou rizikových faktorov pracovného i životného prostredia, prevenciou ochorení, presadzovaním, podporovaním a rozvíjaním činností smerujúcich k ochrane, podpore a rozvoji verejného zdravia.

Hlavnou motiváciou projektu je zvýšenie úrovne KIB, aby RÚVZ so sídlom v Trnave bol lepšie pripravený čeliť interným a externým hrozbám v oblasti KIB. Na rozdiel od súčasného stavu bude disponovať výrazne vyššími schopnosťami detekcie škodlivých aktivít, technologické vybavenie bude umožňovať lepšiu ochranu pred útokmi z externého a interného prostredia, ako aj ochranu dát.

Medzi hlavné **ciele systému riadenia KIB** patria:

- zabezpečenie správnej a bezpečnej prevádzky prostriedkov spracúvajúcich informácie,
- monitorovanie prostredia,

- evidencia a ošetrovanie podozrivých udalostí a bezpečnostných incidentov s dôrazom na prevenciu ich opakovaného výskytu.

Agenda/životná situácia

Predkladaný projekt nie je viazaný na konkrétnu životnú situáciu

Systémy

Medzi kľúčové identifikované CIS v zmysle vyhlášky č. 362/2018 Z.z., ktorých ohrozenie by malo významný vplyv na poskytovanie základnej služby, resp. by výskyt incidentu spôsobil vážny výpadok IS žiadateľa možno zaradiť:

- **MIS registratúra** – ide o administratívny systém úradu, ktorý podporuje IS VS a do ktorého sa zapisujú všetky pokuty, prešetrenia, informácie o PO a FO. Slúži na zdokumentovanie, zasielanie, podpisovanie a prijímanie rozhodnutí a archiváciu informácií.

RÚVZ so sídlom v Trnave sa nahlasuje a zaznamenáva údaje do nasledujúcich ISVS:

- IS úradov verejného zdravotníctva – IS HŽP, IS PPL, IS HV, IS KOZV, IS VnK, IS PV, IS LAB, IS ŠZD, IS OSp, MIS - Registratúra
- IS o kúpaliskách a o kvalite vody na kúpanie
- IS RAPID ALERT: - hlásenie zdravotne škodlivých potravín a premetov na styk s potravinami
- IS RASSF - rýchly výstražný systém pre potraviny a krmivá (Rapid Alert System for Food and Feed – RASFF)
- IS Pitná voda s dočasným úložiskom UVZSR Aktovka
- IS EPIS - sledovanie a analýza výskytu chrípky a surveillance pneumokokových invazívnych ochorení a invazívnych hemofilových nákaz, evidenciu a analýzu prípadov ochorení
- IS prenosných ochorení, Cyanobaktérie
- IS HACCP/SV HACCP (Hazard Analysis and Critical Control Points) je globálne najrozšírenejším systémom zameraným na zaistenie bezpečnosti potravín v celom reťazci
- IT na zabezpečenie dátových SIM kariet v súvislosti so zavedením Integrovaného informačného systému.
- IS v ISÚVZ
- Peľová informačná služba (PIS) podľa zákona č. 355/2007 Z. z. o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
- Národný IS pre sledovanie rezistencie na antibiotiká SNARS SK - http://www.snars.sk.

Vyhlásená výzva č. OPII-PSK-MIRRI-611-2024-DV-EFRR „*Podpora v oblasti KIB na regionálnej úrovni – VS*" súvisí najmä s naplnením povinností:

- definovanými v zákone o KB a v zákone o ITVS,
- opatreniami definovanými v § 20 zákona o KB,
- nutnosť zvýšenia úrovne a schopnosti zabezpečovať a riadiť KIB vzhľadom na sústavne sa zvyšujúce hrozby a riziká,
- zabezpečenie realizácie spoločných blokov bezpečnostnej architektúry v súlade s NKIVS a strategickou prioritou KIB, ako reakcia na aktuálny nedostatočný stav úrovne vyspelosti procesov riadenia KIB, ako reakcia na aktuálne zmeny v používaní IT, ako aj závažné útoky v oblasti KB.

Hlavný popis problému

Aktuálne má RÚVZ Trnava nedostatky v Z. z. 69/2018 a Vyhlášky NBÚ č. 362/2018. Z tohto dôvodu aktuálne úroveň kyberbezpečnosti nespĺňa platnú legislatívu. To môže mať za následok i ohrozenie prevádzky základnej služby – registratúry, pri kyberbezpečnostnom incidente, keďže útočník má aktuálne jednoduchšiu možnosť infiltráciu do siete RÚVZ Trnava a úspešným útokom i prístup k dôverným a interným informáciám, osobných údajom a zdravotnej dokumentácií niektorých občanov. Taktiež pri kyberbezpečnostnom incidente aktuálne môže byť zamedzená kontinuita základnej služby a možnosť zamestnancov vykonávať kontrolu štátneho zdravotného dozoru nad spĺňaním povinnosti subjektov podľa platnej legislatívy v oblasti verejného zdravia v Trnavskom kraji a zamedzenie riadneho prešetrenia chorôb z povolania a otvárania nových prevádzok, či vydávanie odbornej spôsobilosti na základe skúšky občanom. Zvýšenie úrovne kybernetickej bezpečnosti splní platnú legislatívu v oblasti KB a zmenší riziko kyberbezpečnostného útoku, či rádius zasiahnutých služieb v prípade KB incidentu.

Predmetom realizácie projektu bude zavedenie a IT podpora nasledovných procesov:

- riadenie prevádzky siete a IS,
- zaznamenávanie, monitorovanie a riešenie incidentov KB,
- zabezpečovanie kontinuity prevádzky.

Oblasti zamerania projektu

Projekt sa primárne zaoberá oblasťou zabezpečenia opatrení KIB v zmysle zákona o KBI a zákona o ISVS. Ako bude uvedené ďalej, tento projekt má priamy dopad na všetky ISVS a technologické platformy, ktoré sú určené na poskytovanie služieb RÚVZ so sídlom v Trnave, nakoľko výsledky projektu budú ochraňovať všetky IS pred potenciálnymi hrozbami KIB.

Ide najmä o oblasti:

- riadenie rizík KIB,
- personálna bezpečnosť,
- riadenie prístupov,
- bezpečnosť pri prevádzke IS a sietí,
- ochrana proti škodlivému kódu,
- sieťová a komunikačná bezpečnosť,
- zaznamenávanie udalostí a monitorovanie,
- riešenie kybernetických bezpečnostných incidentov,
- kontinuita prevádzky,
- audit, riadenie súladu a kontrolné činností.

Žiadateľ/RÚVZ TT deklaruje, že zrealizuje nasledovné aktivity:

- vytvorí stratégiu kybernetickej bezpečnosti,
- vytvorí bezpečnostné politiky kybernetickej bezpečnosti,
- vykonaná inventarizáciu aktív, klasifikáciu informácií a kategorizáciu sietí a informačných systémov,
- realizuje analýzu rizík a analýzu dopadov spolu, vrátane riadenia rizík.

Rozsah projektu Realizácia projektu sa dotkne nasledovných ISVS prevádzkovaných na úrovni RÚVZ so sídlom v Trnave:

- MIS - Registratúra

Realizácia projektu sa dotkne nasledovných subjektov:

- RÚVZ so sídlom v Trnave,
- interní zamestnanci RÚVZ so sídlom v Trnave,
- externí zamestnanci RÚVZ so sídlom v Trnave,
- poskytovateľ IT služby.

3.3 Zainteresované strany/Stakeholderi

Tabuľka 5 Zainteresované strany/Stakeholderi

ID	**aktér/Stakeholder**	**subjekt** (skratka)	**rola** (vlastník procesu/ vlastník dát/zákazník/užívateľ …. člen tímu atď.)	**IS** (názov ISVS a MetaIS kód)
1	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky	MIRRI	Poskytovateľ	n/a
2	Úrad verejného zdravotníctva Slovenskej republiky	ÚVZSR	vlastník procesu/ vlastník dát/	podávanie informácií cez jednotlivé IS ÚVZ
3	Regionálny úrad verejného zdravotníctva so sídlom v Trnave	RUVZ	vlastník procesu/ vlastník dát/ prevádzkovateľ / užívateľ IS zabezpečuje prevádzku IT	MIS – interná registratúra úradu
4	generálny tajomník služobného úradu	RUVZ	koordinácia aktivít organizačných zložiek RÚVZ pri zavedení interných bezpečnostných smerníc do praxe a riešení otázok KB	MIS – interná registratúra úradu
5	manažér KB	RUVZ	zodpovedný za KB v zmysle smernice S01 v článok 1.3./vlastník procesov	MIS – interná registratúra úradu
6	správca IT	RUVZ	Správca procesov	MIS – interná registratúra úradu
7	zamestnanec	RUVZ	využíva IS v rozsahu primeranom jeho pracovnej pozícii a pracovnej náplne	MIS – interná registratúra úradu

3.4 Ciele projektu

Ciele projektu sú definované v súlade s NKIVS a súčasne sú definované tak, aby boli v súlade s očakávanými výsledkami definovanými v Partnerskej dohode SR na roky 2021 – 2027 (ďalej len „*Partnerská dohoda*“) pre RSO 1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány VS. Partnerská dohoda definuje špecifický cieľ RSO 1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány VS a konkrétne opatrenie: 1.2.1 Podpora v oblasti informatizácie a digitálnej transformácie, oblasť – KIB, kde hlavným cieľom je zvýšenie inovačnej schopnosti ekonomiky, prostredníctvom zavádzania inovatívnych a bezpečných digitálnych technológií, zvýšenie kvality poskytovaných verejných služieb a zabezpečenie KB v súlade so Stratégiou digitálnej transformácie Slovenska 2030. Očakávaným výsledkom je „*zvýšenie úrovne a odolnosti KIB, najmä kritickej infraštruktúry v prostredí VS*“.

Súlad projektu s cieľmi relevantných strategických dokumentov:

Tabuľka 6 Súlad cieľa projektu s cieľmi strategických dokumentov

názov	**popis**
Národná koncepcia informatizácie VS SR (2021)	Projekt je v súlade s Národnou koncepciou informatizácie verejnej správy Slovenskej republiky, Prioritná os 4 Kybernetická a informačná bezpečnosť konkrétne so špecifickým cieľom Zvýšenie schopnosti včasnej identifikácie kybernetických incidentov vo verejnej správe. RÚVZ je zaradené do kritickej infraštruktúry a zabezpečenie spoľahlivého fungovania, a teda aj udržanie úrovne kybernetickej a informačnej bezpečnosti, je nevyhnutným predpokladom zabezpečenia chodu organizácie z hľadiska procesného a zabezpečenia funkčnej prevádzky RUVZ TT. · skracuje na realizáciu projektov, zvyšuje hodnotu nasadených systémov a optimalizuje náklady na prevádzku systémov, · posilňuje ľudské kapacity, minimalizuje bezpečnostné incidenty a škody; zvyšuje úroveň ekosystému kybernetickej a IB.
Chartou základných práv EÚ, zabezpečuje a presadzuje rodovú rovnosť, nediskrimináciu a prístupnosť pre osoby so zdravotným postihnutím (článok 9 a článok 73 ods. 1 nariadenia o spoločných ustanoveniach)	· projekt zabezpečuje dodržiavanie základných práv a súlad s Chartou základných práv EÚ, · v projekte je zohľadňovaná a presadzovaná rovnosť mužov a žien, uplatňuje a začleňuje sa hľadisko rodovej rovnosti, · v projekte sú prijaté opatrenia na zabránenie akejkoľvek diskriminácie, · projekt zabezpečuje a zohľadňuje prístupnosť pre osoby so zdravotným postihnutím.
Zákon č. 69/2018 Z. z. o KB a o zmene a doplnení niektorých zákonov v závislosti od kategórie bezpečnostného incidentu.	· Aktivity projektu sú zamerané na opatrenia a aktivity, ktoré vyšli zo samohodnotenia, ktoré prispievajú ku zvýšeniu úrovne informačnej a kybernetickej bezpečnosti v RUVZ.

Hlavným cieľom je do prostredia RÚVZ so sídlom v Trnave je „*zlepšovanie technologického, procesného, infraštruktúrneho, vedomostného a organizačného zabezpečenia zručností a kapacít pre plnenie úloh v oblasti KIB v prostredí orgánov štátnej a VS*“.

Po implementácii projektu bude proces zavedený a ďalej vykonávaný aj internými zamestnancami, predovšetkým Manažérom KB, a ďalšími oprávnenými zamestnancami.

Hlavným výsledkom realizácie projektu bude realizácia a optimalizácia procesov riadenia kybernetickej bezpečnosti, riadenia rizík, kontinuity činností a riadenia incidentov.

Všetky ciele projektu sú definované v súlade s vyššie uvedenými strategickými dokumentmi.

Spôsob realizácie aktivít projektu

Projekt s je koncipovaný ako súbor opatrení, ktorého predmetom sú nasledovné oblasti:

1. Analýza aktuálneho stavu.
2. Naplnenie technických, organizačných a procesných podmienok.
3. Naplnenie personálnych podmienok na zabezpečenie riadneho chodu RÚVZ so sídlom v Trnave.
4. Technologické zabezpečenie.

Tieto oblasti predstavujú nákup HW a SW a budú realizované prostredníctvom aktivity Obstaranie HW/SW/OS. Inštalačné práce, konfigurácia a ladenie sú súčasťou dodávky samostatného HW a SW.

Implementácia projektu bude pozostávať z nasledovných aktivít:

A1: Analýza a Dizajn

1.1 Konzultačné a analytické práce

1.2 Identifikácia možností realizácie, potrebných zdrojov a riešení

1.3 Identifikácia a analýza rolí, procesov a integrácií

1.4 Funkčná a nefunkčná špecifikácia celého riešenia

1.5 Definícia všetkých bezpečnostných a špecializovaných produktov spolu s akceptačnými kritériami

1.6 Vykonanie analýz bezpečnosti a súladu s požiadavkami zákona o KB a návrh najmä organizačných a procesných bezpečnostných opatrení na dosiahnutie súladu

Výstupom bude:

- identifikovanie a analýza poskytovaných služieb a IS,
- aktualizovanie zoznamu a informačných aktív,

Za účelom zabezpečenia súladu s požiadavkami zákona o KB budú vykonané aj ďalšie analýzy bezpečnosti a súladu s požiadavkami zákona o KB. Na základe ich výsledku budú navrhnuté najmä organizačné a procesné bezpečnostné opatrenia, ktoré budú realizované v rámci A1. Implementácia.

A2: Obstaranie HW/SW/OS:

2.1 Nákup HW a SW rozširujúceho funkcionalitu existujúceho IS

2.2 Nákup HW a SW Deduplikačné zálohovacie úložisko

Výstupom bude:

- Obstaraný HW a SW (licencie)

A3: Implementácia a Testovanie

3.1 Zavedenie a konfigurácia zariadení a integrácia do siete úradu.

3.2 Integrácia MIS - registratúry s novou konfiguráciou na sieti.

3.3 Inštalácia kyberbezpečnostných zariadení do siete RÚVZ so sídlom v Trnave.

3.4 Príprava a úprava kyberbezpečnostnej dokumentácie kvôli zmene zariadení na sieti.

3.5 Obvyklé testovanie a ladenie riešení popri ich implementácii.

3.6 Konfigurácia segmentácie, testovanie a ladenie riešenia.

3.7 Testovanie funkcionality riešenia.

3.8 Testovanie zraniteľností a „case-hardening“.

3.9 Testovanie integrácií.

3.10 Testovanie pilotnej prevádzky.

3.11 Akceptačné testovanie.

Výstupom bude:

- Akceptačný protokol

A4: Nasadenie a monitorovanie:

4.1 Nasadenie riešenia do produkčného prostredia.

4.2 Zadefinovanie testovacích a tréningových podkladov a materiálov pre testovanie bezpečnostných záplat a konfigurácií a zvyšovanie bezpečnostného povedomia.

4.3 Prechod na plnú prevádzku.

Výstupom bude:

- Akceptačný protokol

5 - Podpora prevádzky (SLA)

Na základe podpísanej zmluvy s dodávateľom HW a SW licencia so zárukou na dodané sieťové zariadenia a záruka na dodané služby - počet rokov podľa zmluvy.

Podporná aktivita – nepriame výdavky:

V rámci tejto podaktivity pôjde o činnosti, ktoré nebudú môcť byť prepojené priamo na konkrétnu činnosť projektu.

- Riadenie projektu.
- Publicita projektu.
- Realizované VO - prieskum trhu.

3.5 Merateľné ukazovatele (KPI)

Projektom budú naplnené nasledujúce ciele a identifikované MU:

Tabuľka 7 MU / KPI projektu

ID	ID/Názov cieľa	Názov ukazovateľa (KPI)	**MJ**	**AS-IS MERATEĽNÉ VÝKONNOSTNÉ HODNOTY** (aktuálne)	**TO-BE MERATEĽNÉ VÝKONNOSTNÉ HODNOTY** (cieľové hodnoty projektu)	**SPÔSOB ICH MERANIA/ OVERENIA PO NASADENÍ** (overenie naplnenie cieľa)	**čas plnenia**	**typ závislosti MU projektu**	**príznak rizika**	**Relevancia k HP**
PO095 / PSK PSOI 12	Zlepšovanie technologického, procesného, infraštruktúrneho, vedomostného a organizačného zabezpečenia zručností a kapacít pre plnenie úloh v oblasti KIB v prostredí orgánov štátnej a VS	Verejné inštitúcie podporované v rozvoji kybernetických služieb, produktov a procesov	verejné inštitúcie	0	1	Akceptačný protokol Projekt implementuje nástroje do celej siete	ku koncu realizácie hlavných aktivít projektu	Max. hodnota	nie	áno
PR017 / PSK PRCR11	Zlepšovanie technologického, procesného, infraštruktúrneho, vedomostného a organizačného zabezpečenia zručností a kapacít pre plnenie úloh v oblasti KIB v prostredí orgánov štátnej a VS	Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov	používatelia / rok	0	1	Akceptačný protokol Projekt implementuje nástroje do celej siete	v rámci udržateľnosti projektu	Max. hodnota	nie	áno

3.6 Špecifikácia potrieb koncového používateľa

n/a

Cieľom prekladaného projektu nie je zlepšenie služieb, ale predovšetkým zabezpečenie jeho ďalšej, udržateľnej prevádzky aj po ukončení doby udržateľnosti projektu.

3.7 Riziká a závislosti

Medzi **riziká s vysokou závažnosťou** RÚVZ so sídlom v Trnave zaraďuje:

ID6 C&C vírus – s vysokou závažnosťou vzniku a významným dopadom - ktorý bude mať za následok infiltrácia do koncových staníc.

Medzi **riziká so strednou závažnosťou** RÚVZ so sídlom v Trnave zaraďuje:

- **ID1** Nedostatočná dátová priepustnosť LAN sieťou
- **ID3** Technické chyby sieťových služieb, technické chyby užívateľskej stanice, ktorá spracováva údaje
- **ID4** Nefunkčnosť zálohovacie systému

- so strednou závažnosťou vzniku, ale s a významným dopadom – ktoré budú mať za následok nefunkčnosť systému, stratu údajov a kritických údajov.

Podiel vysoko-závažných rizík (A1, A2, B1) tvorí: menej ako 16,67 %.

Detailný popis rizík a závislostí sa nachádza v Prílohe č. 1 tohto dokumentu.

3.8 Stanovenie alternatív v biznisovej vrstve architektúry

V zmysle Vyhlášky č. 401/2023 Z.z. o riadení projektov a zmenových požiadaviek v prevádzke IT VS pre časť ALTERNATÍVY A MCA nie sú stanovené alternatívy.

Zdôvodnenie

- Zachovanie pôvodného stavu nie je riešením z dôvodu nedostatku úrovne kybernetickej bezpečnosti a aktuálne i nespĺňania povinností vyplývajúcich zo Z. z. 69/2018 a Vyhlášky NBÚ.
- Migrovanie registratúry do siete ÚVZ nie je možné z dôvodu rýchlosti linky, keďže všetky úrady sú sieťovo prepojené a v iných lokalitách a pristupovanie všetkých úradov by ovplyvnilo rýchlosť linky a efektivitu práce.
- Zanechanie registratúry a zvýšenie úrovne kybernetickej bezpečnosti a splnenie povinností vyplývajúcich zo Z. z. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

3.9 Multikriteriálna analýza

n/a

3.10 Stanovenie alternatív v aplikačnej vrstve architektúry

n/a

4. POŽADOVANÉ VÝSTUPY (PRODUKT PROJEKTU)

Predkladaný projektový zámer nemá za ciel meniť procesy, len znížiť náklady na prevádzku a zabezpečiť udržateľnosť riešenia.

Z pohľadu výstupov je projekt budovaný prostredníctvom 1 inkrementu, keďže pre splnenie cieľov projektu je nevyhnutné realizovať dodanie výstupov súčasne. Implementácia projektu prechádza štandardnými fázami riadenia IT projektov uvedených v podkapitole **3.4 CIELE PROJEKTU A MU**, v časti **Spôsob realizácie aktivít projektu**.

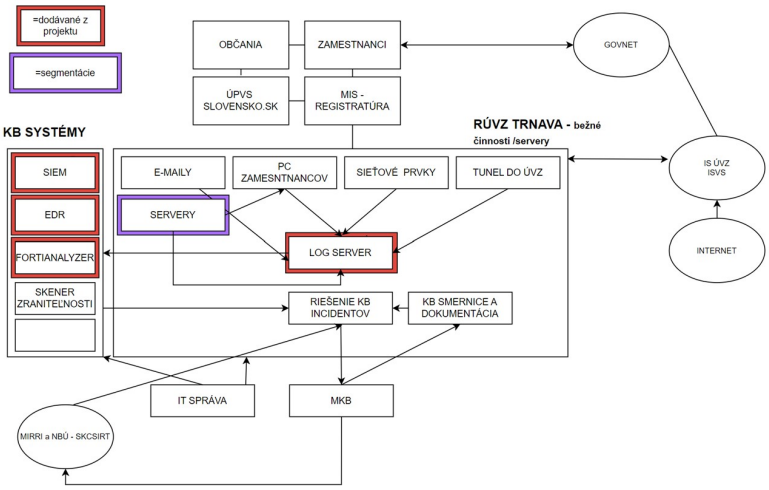
Pre tieto fázy/aktivity sú definované výstupy, ktoré majú byť dodané a budú predmetom akceptačných kritérií/protokolov

Z hľadiska plnenia cieľov projektu bude výsledkom projektu naplnenie hlavného cieľa, t.j. súlad KIB so zákonom o KB a so zákonom o ISVS, čo bude naplnené realizáciu nasledovných partikulárnych cieľov:

- riadenie rizík KIB,
- personálna bezpečnosť,
- riadenie prístupov,
- bezpečnosť pri prevádzke IS a sietí,
- ochrana proti škodlivému kódu,
- sieťová a komunikačná bezpečnosť,
- zaznamenávanie udalostí a monitorovanie,
- riešenie kybernetických bezpečnostných incidentov,
- kontinuita prevádzky,
- audit, riadenie súladu a kontrolné činností.

Vlastníkom produktov bude RÚVZ TT. Procesné a projektové riadenie vrátane popisu rolí a zodpovedností je v 9 Projektový tím.

5. NÁHĽAD ARCHITEKTÚRY



Obrázok 1 Náhľad architektúry

5.1 Prehľad e-Government komponentov

n/a

6. LEGISLATÍVA

Projekt nevyžaduje zmeny legislatívy.

Projekt je realizovaný za účelom dosiahnutia súladu s platnou legislatívou, a to najmä:

- Zákon 69/2018 Z.z. (NBÚ) o KB (od 30.1.2018),

- Zákon 95/2019 Z.z. o IT VS (od 27.3.2019),
- Zákon 576/2004 Z.z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov
- Zákon 355/ 2007 o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov
- Vyhláška č.78/2020 Z.z. o štandardoch pre ITVS (od 1.5.2020),
- Vyhláška č.85/2020 Z.z. o riadení projektov (od 1.5.2020 do 14.11.2023),
- Vyhláška č.401/2023 Z.z. o riadení projektov a zmenových požiadaviek v prevádzke IT VS (od 15.11.2023),
- Vyhláška 179/2020 Z.z. o obsahu bezpečnostných opatrení IT VS (od 30.6.2020),
- Vyhláška 362/2018 Z.z. o obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (od 11.12.2018),
- Vyhláška 547/2021 Z.z. (UX/IDSK) o elektronizácii agendy VS (od 1.1.2022).

Projekt je v súlade s o zákonom 578 z 21. októbra 2004

o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve a o zmene a doplnení niektorých zákonov

§ 80

Povinnosti zdravotníckeho pracovníka

(2) Zdravotnícky pracovník je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvedel v súvislosti s výkonom svojho povolania.

(3) Povinnosti mlčanlivosti môže zdravotníckeho pracovníka zbaviť iba osoba, ktorej sa skutočnosti týkajú, alebo orgán príslušný na vydanie povolenia, a to na žiadosť orgánov činných v trestnom konaní a súdov.

(4) Povinná mlčanlivosť sa neporuší postúpením zdravotnej dokumentácie medzi lekármi poskytujúcimi zdravotnú starostlivosť, ako aj v ďalších prípadoch ustanovených osobitným predpisom.59)

(5) Povinná mlčanlivosť sa neporuší ani informovaním

1. a) zdravotníckeho pracovníka, ak rozsah poskytovanej informácie nepresahuje rámec informácií, ktoré zdravotnícky pracovník nevyhnutne potrebuje na riadne plnenie úloh pri poskytovaní zdravotnej starostlivosti,
2. b) členov a pracovníkov komôr pri vykonávaní tých právomocí a v takom rozsahu, ktoré im priznáva tento zákon.

(6) Povinnosť oznamovať určité skutočnosti uložené zdravotníckemu pracovníkovi osobitnými predpismi60) týmto nie je dotknutá. Ten, komu sa skutočnosti oznamujú, je povinný zachovávať o nich mlčanlivosť.

Zákon 576 z 21. októbra 2004

o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov

§ 24

Poskytovanie údajov zo zdravotnej dokumentácie

(1) Údaje zo zdravotnej dokumentácie podľa § 20 ods. 2 a 3 sa poskytujú formou výpisu zo zdravotnej dokumentácie podľa § 20 ods. 2 a 3. Výpis zo zdravotnej dokumentácie podľa § 20 ods. 2 a 3 obsahuje okrem údajov uvedených v § 19 ods. 2 písm. a), h) a i)

(4) Poskytovateľ je povinný na základe písomného vyžiadania, ak v písmene a) nie je ustanovené inak, bezodkladne poskytnúť výpis zo zdravotnej dokumentácie v rozsahu, ktorý priamo súvisí s účelom vyžiadania,

1. e) osobám oprávneným nahliadať do zdravotnej dokumentácie, ak rozsah vyžiadania nepresahuje rozsah sprístupňovania údajov zo zdravotnej dokumentácie týmto osobám podľa § 25 ods. 1, a ak nie je týmto osobám zakázané poskytovanie údajov zo zdravotnej dokumentácie podľa § 18 ods. 4; ustanovenie § 25 ods. 8 sa použije primerane,

§ 25

Sprístupňovanie údajov zo zdravotnej dokumentácie

(1) Osoba je oprávnená udeliť súhlas na prístup k údajom zo svojej elektronickej zdravotnej knižky v rozsahu a spôsobom ustanovenom osobitným predpisom.31b) Údaje zo zdravotnej dokumentácie podľa § 20 ods. 2 a 3 sa sprístupňujú bezodkladne formou nahliadania do zdravotnej dokumentácie osoby

1. n) odbornému pracovníkovi epidemiológie príslušného regionálneho úradu verejného zdravotníctva a odbornému pracovníkovi epidemiológie úradov verejného zdravotníctva Ministerstva vnútra Slovenskej republiky a Ministerstva obrany Slovenskej republiky v rozsahu potrebnom na zabezpečenie epidemiologického vyšetrovania,

7. ROZPOČET A PRÍNOSY

S ohľadom na rozpočet projektu (projekt do 1.000.000,00 €) nebola spracovaná **Analýza nákladov a prínosov**.

V uvedenom projekte vychádzame pri stanovení rozpočtu z prieskumu trhu a pravidiel stanovených uvedenou Výzvou.

Tabuľka 8 Rozpočet projektu

skupina výdavkov	názov výdavku	MJ	počet	JC bez DPH	Suma s DPH	NFP	prieskum trhu
PRIAME VÝDAVKY							
518	Bezpečnostná dokumentácia	projekt	1	28 633,33 €	34 360,00 €	34 360,00 €	Určenie PHZ e-mailom, na základe informácií z webu alebo predchádzajúceho plnenia – identifikácia oslovených subjektov a zistených indikatívnych cien zo dňa 24.06.2024
022	Segmentácia siete	projekt	1	44 441,00 €	53 329,20 €	53 329,20 €	Určenie PHZ e-mailom, na základe informácií z webu alebo predchádzajúceho plnenia – identifikácia oslovených subjektov a zistených indikatívnych cien zo dňa 24. – 25. 06.2024
022	Implementácia nástroja na sledovanie a detekciu prevádzky	projekt	1	50 128,67 €	60 154,40 €	60 154,40 €	Určenie PHZ e-mailom, na základe informácií z webu alebo predchádzajúceho plnenia – identifikácia oslovených subjektov a zistených indikatívnych cien zo dňa 24. – 25. 06.2024
022	Implementácia centralizovaného systému ochrany pred škodlivým kódom	kus	1	50 011,00 €	60 013,20 €	60 013,20 €	Určenie PHZ e-mailom, na základe informácií z webu alebo predchádzajúceho plnenia – identifikácia oslovených subjektov a zistených indikatívnych cien zo dňa 24. – 25. 06.2024
022	Bezpečnostné zálohovacieho úložisko	kus	1	67 776,00 €	81 331,20 €	81 331,20 €	Určenie PHZ e-mailom, na základe informácií z webu alebo predchádzajúceho plnenia – identifikácia oslovených subjektov a zistených indikatívnych cien zo dňa 24. – 25. 06.2024
NEPRIAME VÝDAVKY							
907	Paušálne výdavky	projekt	1	--	20 243,16	20 243,16	---
CELKOVÁ VÝŠKA OPRÁVNENÝCH VÝDAVKOV					**309 431,16 €**		

V prípade projektov KB je priame vyčíslenie návratnosti pomerne komplikované. Z pohľadu návratnosti je potrebné venovať sa hodnoteniu možných škôd, ktoré by vznikli v prípade, že nebude adekvátne riešená KIB. Ide o nasledovné potenciálne škody:

Finančné riziko – dôsledky kybernetického útoku. Ide o možné sankcie vyplývajúce priamo z legislatívnych rámcov, prípadných súdnych sporov (v prípade napríklad úniku osobných údajov) ako aj nákladov spojených so sanáciou prípadného kybernetického incidentu. Tieto finančné prostriedky nie je možné momentálne vyčísliť, reálne však môže niekoľko násobne prekročiť straty interných finančných prostriedkov RÚVZ so sídlom v Trnave.

Reputačné riziko – vzhľadom na postavenie a oblasť spoločenskej dôležitosti a zákonných povinností RÚVZ so sídlom v Trnave, je toto riziko potenciálne vysoké – teda v prípade neplnenia legislatívnych požiadaviek v zmysle zákona o KB a zákona o ISVS alebo vyhlášky 362 /2018 Z. z. či reálneho výpadku prevádzky základnej služby, úniku citlivých dát v a pod.

Sumarizácia nákladov a prínosov

Tabuľka 9

Náklady	Bezpečnostná dokumentácia	Segmentácia siete	EDR+SIEM
Všeobecný materiál	34 360,00	53 329,20	201 498,80
IT - CAPEX	**34 360,00**	53 329,20	**99 500**
Práca	*34 360,00*	*12 265*	*40 300*
SW	*0*	*14 400*	*50 375*
HW	*0*	*26 664*	*110 823*

IT - OPEX- prevádzka ročne	**0**	**700**	**1200**
Práca	*0*	*400*	*1000*
SW	*0*	*0*	*0*
HW	*0*	*300*	*200*
Prínosy			
Finančné prínosy			
Administratívne poplatky	*0*	*0*	*0*
Ostatné daňové a nedaňové príjmy	*0*	*0*	*0*
Ekonomické prínosy			
Občania (€)	*0*	*0*	*0*
Úradníci (€)	*0*	*0*	*0*
Úradníci (FTE)	*0*	*0*	*0*
Kvalitatívne prínosy			
	Bezpečnostné postupy	*Zvýšenie KB*	*Zvýšenie KB*

Kvalitatívne prínosy projektu

- Efektívna a spoľahlivá ochrana citlivých informácií a dát
- Znížené riziko výpadkov a nedostupnosti systému
- Zvýšenie spokojnosti oprávnených zamestnancov s prácou na MIS registratúre

8. HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU a METÓDA JEHO RIADENIA

Tabuľka 9 Harmonogram

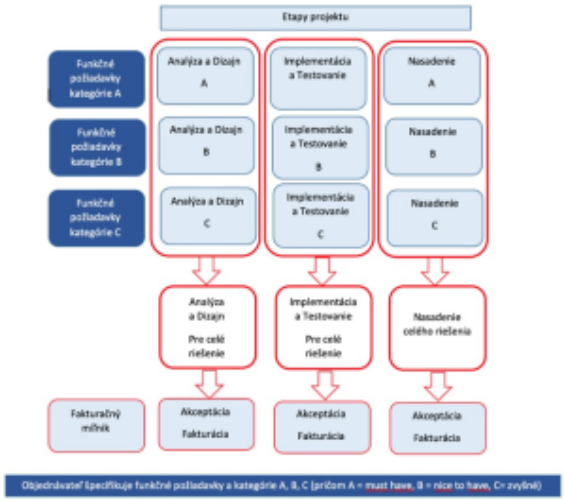
ID	fáza / etapa / aktivita	predpokladaný začiatok	predpokladaný koniec	poznámka
1	Prípravná fáza	3/2024	12/2024	· príprava procesov VO
2	Iniciačná fáza	9/2024	12/2024	· podpísanie Zmluvy o NFP · spustenie procesov VO
3	Realizačná fáza	01/2025	11/2025	· podpísanie zmlúv s dodávateľmi po ukončení VO · realizácia projektu
A1	Analýza a Dizajn	01/2025	05/2025	
A2	Obstaranie HW /SW/OS	02/2025	08/2025	
A3	Implementácia a Testovanie	08/2025	10/2025	· minimálne 2 mesiace testovacej prevádzky
A4	Nasadenie a monitorovanie	10/2025	11/2025	
4	Dokončovacia fáza	10/2025	12/2025	· počas dokončovacej fázy projektový manažér pripraví podklady a odovzdá na schválenie záverečnú žiadosť o platbu a záverečnú monitorovaciu správu
5	Podpora prevádzky (SLA)	01/2026	01/2031	· obdobie udržateľnosti

Z hľadiska procesného riadenia projektu podľa vyhlášky č. 401/2023 MIRRI SR z 9. októbra 2023 o riadení projektov a zmenových požiadaviek v prevádzke ITVS, bude projekt riadený na základe princípu **WATERFALL – VODOPÁDOVÝ PRÍSTUP**.

Waterfall – vodopádový prístup počíta s detailným naplánovaním jednotlivých krokov a následnom dodržiavaní postupu pri vývoji alebo realizácii projektu. Projektovému tímu je daný minimálny priestor na zmeny v priebehu realizácie. Vodopádový prístup je vhodný a užitočný v projektoch, ktorý majú jasný cieľ a jasne definovateľný postup a rozdelenie prác.

Objednávateľ projektu vypracuje **funkčnú špecifikáciu - detailnú** a **technickú špecifikáciu - rámcovú**.

Schéma princípu projektového riadenia:



9. PROJEKTOVÝ TÍM

RÚVZ so sídlom v Trnave disponuje s dostatočnou kapacitou pre riadenie a prevádzku projektu.

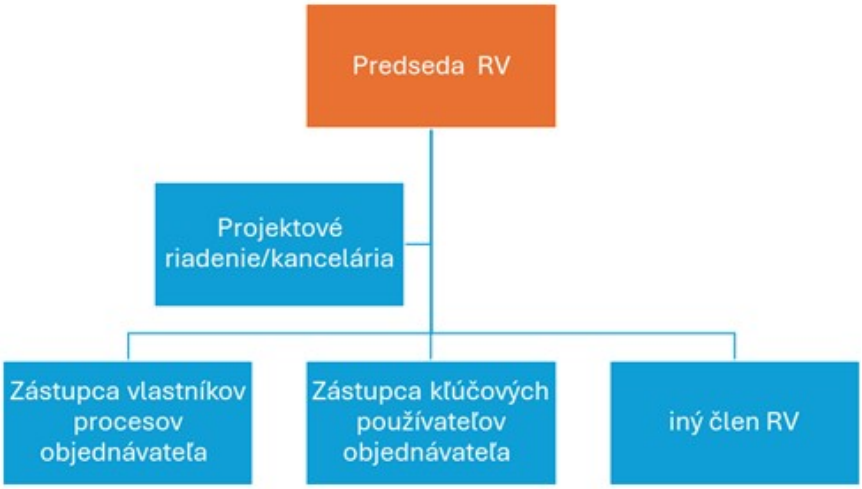
Pre účely realizácie projektu sa zostavuje RV, v minimálne nasledovnom zložení:

- Predseda RV – Mgr. Tomáš Hauko, MPH.
- Zástupca vlastníkov procesov objednávateľa - Denis Dojčan.
- Zástupca kľúčových používateľov objednávateľa - bude stanovené po podpise Zmluvy o NFP.
- Projektový manažér - bude stanovené po podpise Zmluvy o NFP.

Tabuľka 10 Role v projekte

ID	Meno a Priezvisko	Pozícia	Organizácia	Oddelenie	Rola v projekte
1	Mgr. Tomáš Hauko, MPH	Generálny tajomník služobného úradu	interný zamestnanec RÚVZ so sídlom v Trnave	Útvar regionálneho hygienika a generálneho tajomníka služobného úradu	Predseda RV
2	Denis Dojčan	Manažér KB	interný zamestnanec RÚVZ so sídlom v Trnave	Útvar regionálneho hygienika a generálneho tajomníka služobného úradu	Zástupca vlastníkov procesov objednávateľa
3	bude stanovené po podpise Zmluvy o NFP	Správca IT	interný zamestnanec RÚVZ so sídlom v Trnave	n/a	Zástupca kľúčových používateľov objednávateľa
4	bude stanovené po podpise Zmluvy o NFP	bude stanovené po podpise Zmluvy o NFP	--	n/a	Projektový manažér

Vzor organizačnej štruktúry



10. PRACOVNÉ NÁPLNE

Z hľadiska procesného riadenia projektu podľa vyhlášky č. 401/2023 Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky z 9. októbra 2023 o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy, bude projekt riadený na základe princípu waterfall.

RÚVZ so sídlom v Trnave disponuje s dostatočnou kapacitou pre riadenie a prevádzku projektu.

Pre účely realizácie projektu sa zostavuje RV, v minimálne nasledovnom zložení:

- Predseda RV – Mgr. Tomáš Hauko, MPH
- Zástupca vlastníkov procesov objednávateľa - Denis Dojčan
- Zástupca kľúčových používateľov objednávateľa - bude doplnené po podpise Zmluvy o NFP

RV

Práva a povinnosti členov RV:

- Právo a povinnosť zúčastňovať sa na zasadnutiach RV.
- Právo uplatniť si pripomienky, podávať podnety alebo vyjadriť sa k pracovnému materiálu predloženému na zasadnutí RV alebo v rámci dištančného hlasovania.
- Právo podávať návrhy a podnety týkajúce sa činnosti RV.
- Právo nahliadať do projektovej dokumentácie.
- Navrhovať zmeny Štatútu.
- Iné práva v zmysle Štatútu.
- Zachováva mlčanlivosť o všetkých skutočnostiach pri výkone svojej funkcie aj po ukončení realizácie projektu.

Predseda RV

Povinný člen RV, ktorý má hlasovacie právo – jeden hlas a ktorého hlas má v prípade rovnosti hlasov hodnotu dvoch hlasov.

- Predseda menuje členov RV na návrh inštitúcie, ktorú člen zastupuje.
- Zvoláva a vedie Zasadnutia RV.

Hlavným záujmom a zodpovednosťou predsedu RV je zastupovať záujmy objednávateľa v projekte, kontrolovať súlad projektu a projektových cieľov so strategickými cieľmi, zabezpečiť a udržať finančné krytie (rozpočet) realizácie projektu a zabezpečiť nákladovo prijateľný prístup.

Zástupca vlastníkov procesov objednávateľa

Povinný člen RV, ktorý má hlasovacie právo – jeden hlas.

Hlavným záujmom a zodpovednosťou zástupcu vlastníkov procesov objednávateľa je:

- Schválenie funkčných a technických požiadaviek, potreby, obsahu a prínosov projektu.
- Definovanie očakávaní na kvalitu projektu, kritérií kvality projektových produktov, prínosov pre koncových používateľov a požiadaviek na bezpečnosť.
- Definovanie merateľných výkonnostných ukazovateľov projektov a prvkov.
- Schválenie akceptačných kritérií.
- Akceptácia rozsahu a kvality dodávaných projektových výstupov pri dosiahnutí platobných míľnikov.
- Odsúhlasenie spustenia výstupov projektu do produkčnej prevádzky a dostupnosť ľudských zdrojov alokovaných na realizáciu projektu.

Zástupca kľúčových používateľov objednávateľa

Povinný člen RV, ktorý má hlasovacie právo – jeden hlas. Reprezentuje záujmy budúcich používateľov projektových produktov alebo projektových výstupov. Hlavným záujmom a zodpovednosťou zástupcu kľúčových používateľov je:

- Návrh a špecifikácia funkčných a technických požiadaviek, potreby, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu, požiadaviek koncových používateľov na prínos systému a požiadaviek na bezpečnosť.
- Návrh a definovanie akceptačných kritérií.
- Akceptačné testovanie a návrh na akceptáciu projektových produktov alebo projektových výstupov a návrh na spustenie do produkčnej prevádzky. Predkladanie požiadaviek na zmenu funkcionalít produktov.

Projektový manažér

Zodpovedá za:

- Riadenie projektu počas jeho celého životného cyklu.
- Riadi projektové zdroje, zabezpečuje tvorbu obsahu, odôvodňovanie projektu a predkladá vstupy na rokovanie RV.
- Zodpovedá za riadenie všetkých zdrojov, členov projektového tímu objednávateľa a za efektívnu komunikáciu s dodávateľom alebo stanovenými zástupcami dodávateľa.
- Ďalej zodpovedá za riadenie projektu – stanovenie cieľov, spracovanie a sledovanie dodržiavania harmonogramu prác a rozpočtu, hodnotenie a prezentáciu výsledkov a za riadenie s tým súvisiacich rizík.
- Vedie špecifikáciu a implementáciu projektu v súlade s firemnými štandardami, zásadami a princípmi projektového riadenia.
- Zodpovedá za plnenie projektových cieľov v rámci stanovených kvalitatívnych, časových a rozpočtových plánov a za riadenie s tým súvisiacich rizík.
- Podieľa na plánovaní a vyjednávaní a je hlavnou kontaktnou osobou pre zákazníka.

Kľúčový používateľ (end user)

Zodpovedný za:

- Reprezentáciu záujmov budúcich používateľov projektových produktov alebo výstupov a za overenie kvality produktu.
- Taktiež zodpovedá za návrh a špecifikáciu funkčných a technických požiadaviek, potreby, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu, požiadaviek koncových používateľov na prínos systému a požiadaviek na bezpečnosť.
- Navrhuje a definuje akceptačné kritériá, je zodpovedný za akceptačné testovanie a návrh na akceptáciu projektových produktov, výstupov a návrh na spustenie do produkčnej prevádzky.
- Predkladá požiadavky na zmenu funkcionalít produktov a je súčasťou Projektového tímu.
- Zabezpečuje jednoznačnú špecifikáciu požiadaviek na jednotlivé projektové výstupy (špecializované produkty a výstupy, požiadavky na bezpečnosť...) z pohľadu vecno-procesného a legislatívy, vytvorenie špecifikácie, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu.
- Navrhuje a definuje akceptačné kritériá.
- Vykoná používateľské testovanie funkčného používateľského rozhrania (UX) a finálne odsúhlasenie.
- Vykoná akceptačné testovanie (UAT) a finálne odsúhlasenie.
- Finálny návrh na spustenie do produkcie.
- Predkladá požiadavky na zmenu funkcionalít produktov.

Z hľadiska interného riadenia projektu je odborné zabezpečenie stanované v Bezpečnostnej smernici.

Za kybernetickú bezpečnosť zodpovedajú:

- generálny tajomník služobného úradu,
- manažér kybernetickej bezpečnosti,
- správca informačných technológií,
- všetky oprávnené osoby v rozsahu svojich pracovných kompetencií, ktoré im vyplývajú z ich pracovnej náplne.

Za zabezpečenie vypracovania bezpečnostnej dokumentácie v súlade o zákonom č. 69/2018 Z.z. a zabezpečenie implementácie bezpečnostných opatrení zodpovedá generálny tajomník služobného úradu.

Za dodržiavanie interných bezpečnostných smerníc RÚVZ so sídlom v Trnave zodpovedajú všetci zamestnanci v rozsahu primeranom ich pracovnej pozícii a pracovnej náplne.

Generálny tajomník služobného úradu

Je štatutárnym zástupcom RÚVZ so sídlom v Trnave ako prevádzkovateľa základnej služby.

Schvaľuje bezpečnostnú dokumentáciu RÚVZ so sídlom v Trnave vypracovanú v súlade so zákonom č. 69/2018 Z.z. a v rozsahu podľa vyhlášky č. 362 /2018 Z.z..

Poskytuje podporu a súčinnosť manažérovi KB pri riešení otázok súvisiacich s KB.

Vytvára podmienky pre efektívne presadzovanie zásad bezpečnostnej politiky a jej dodržiavanie zamestnancami RÚVZ so sídlom v Trnave.

V prípade vzniku závažných kybernetických incidentov v spolupráci s manažérom KB zasiela hlásenia o bezpečnostných incidentoch NBÚ SR.

Manažér KIB

Vymenúva generálny tajomník služobného úradu. Pri výbere osoby manažéra KB prihliada predovšetkým na jeho odborné znalosti v oblasti IT so zameraním na otázky KB, najmä schopnosti odhaľovať zraniteľnosti informačných aktív a tiež na znalosti legislatívy v oblasti KB a štandardov pre ISVS. Je priamym podriadeným generálnemu tajomníkovi služobného úradu; v zmysle zákona č. 69/2018 Z.z. a je oprávnený predkladať návrhy a oznamovať informácie v oblasti KB priamo generálnemu tajomníkovi služobného úradu. Má možnosť predkladať mu návrhy a oznamovať informácie v oblasti KB. Zabezpečuje aplikáciu bezpečnostných opatrení v systéme riadenia KB. Je nezávislý od riadenia prevádzky a vývoja služieb IT.

Povinnosti:

- vykonávať poučenie oprávnených osôb zamestnancov RÚVZ so sídlom v Trnave v oblasti KB,
- riešiť a viesť evidenciu o kybernetických bezpečnostných incidentoch,
- navrhovať preventívne opatrenia na opakovanie vyskytnuvším sa a predchádzanie novým bezpečnostným incidentom,
- informovať generálneho tajomníka o výsledku revízie bezpečnostnej dokumentácie; predkladá návrhy na odstránenie zistených nedostatkov,
- 1x ročne vykonávať revíziu bezpečnostnej dokumentácie (kontrola súladu s aktuálnymi podmienkami súvisiacimi s výkonom základných služieb s platnou legislatívou – najmä zákonom č. 69/2018 Z.z. a vyhláškou 362/2018 Z.z.),
- informovať generálneho tajomníka služobného úradu o výsledku revízie bezpečnostnej dokumentácie,
- v závislosti na výsledku revízie bezpečnostnej dokumentácie alebo v prípade zmeny legislatívy súvisiacej s KB vykonávať aktualizáciu bezpečnostnej dokumentácie,
- poskytovať súčinnosť RÚVZ so sídlom v Trnave v konaní s dodávateľmi služieb súvisiacich s prevádzkou základnej služby RÚVZ so sídlom v Trnave,
- poskytovať súčinnosť RÚVZ so sídlom v Trnave v konaní s NBÚ SR.

Správca IT

Rozsah činností:

- navrhuje a realizuje zmeny a technické riešenia s cieľom optimalizácie využitia IS,
- vykonáva inštalácie programov a prostriedkov IT a aktualizácie programového vybavenia,
- vykonáva kontrolu nainštalovaného programového vybavenia na pracovných staniciach a na základe zisteného stavu vypracováva konkrétny návrh na jeho prípadnú obnovu alebo legalizáciu,
- vykonáva preventívne profylaktické prehliadky a zabezpečuje opravy HW,
- vykonáva technickú podporu používateľom – oprávneným osobám,
- zabezpečuje zálohovanie a archiváciu chránených údajov,
- zabezpečuje spoľahlivú prevádzku programového vybavenia,
- v prípade zlyhania alebo obmedzenia funkčnosti automatizovaného IS zabezpečuje jeho obnovu.

Základné povinnosti:

- vykonávať všetky činnosti súvisiace s plnením úloh správcu IT svedomito a odborne podľa svojich najlepších schopností a vedomostí,
- pri plnení pracovných úloh postupovať v súlade s vnútornými predpismi RÚVZ so sídlom v Trnave,
- zachovávať mlčanlivosť o všetkých skutočnostiach, s ktorými prichádza do styku pri plnení svojich povinností,
- sledovať vývoj v oblasti IT a vzdelávať sa,
- pri návrhu a budovaní technickej infraštruktúry IS zvažovať bezpečnostné hrozby pôsobiace na jednotlivé časti automatizovaných IS a závažnosť vplyvu na ich bezpečnosť a spoľahlivosť.

Oprávnené osoby pri práci s informačnými aktívami

Základné povinnosti:

- chrániť zverené informačné aktíva pred stratou, poškodením, odcudzením, zneužitím na iný účel ako boli získané, sprístupnením, poskytnutím nepovolaným osobám alebo inými neprípustnými formami spracúvania, dodržiavať podľa § 12 ods. 1 zákona č. 69/2018 Z.z. mlčanlivosť o všetkých skutočnostiach ktoré musia zostať dôverné, týkajúcich sa prevádzky základnej služby RÚVZ s ktorými prídu do styku v rámci svojho pracovného pomeru, a to aj po ukončení pracovného pomeru voči RÚVZ;
- povinnosť mlčanlivosti sa nevzťahuje na prípady poskytovania súčinnosti v prípade plnenia úloh súdov a orgánov činných v trestnom konaní podľa osobitného zákona alebo vo vzťahu k NBÚ SR pri plnení jeho úloh podľa zákona č. 69/2018 Z.z., prípadne voči Úradu na ochranu osobných údajov pri plnení jeho úloh podľa zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej aj „*oprávnené subjekty*“). V odôvodnených prípadoch môže oprávnenú osobu zbaviť povinnosti mlčanlivosti aj generálny tajomník služobného úradu v súlade s ustanovením §12 ods. 2 písm. b) zákona č. 69/2018 Z.z., najmä v súvislosti s riešením otázok kybernetickej bezpečnosti; ustanovenia vyššie uvedených právnych predpisov o povinnosti mlčanlivosti tým nie sú dotknuté.

V prípade kontroly vykonávanej oprávnenými subjektmi podľa osobitných právnych predpisov sú oprávnené osoby povinné najmä:

- poskytnúť potrebnú súčinnosť pri výkone kontroly, strpieť overenie totožnosti kontrolným orgánom, zdržať sa konania, ktoré by viedlo k mareniu úradného výkonu kontroly.

Ide o interných, resp. externých zamestnancov RÚVZ so sídlom v Trnave.

11. ODKAZY

Odkaz na projekt a príslušnú dokumentáciu v META IS: projekt_2800_Projektovy_zamer_detailny

12. PRÍLOHY

Príloha :

1. P_01_a_I_01_a_M_02_1_PRILOHA_1_REGISTER_RIZIK-a-ZAVISLOSTI_RUVZ_01072024_V2