PROJEKTOVÝ ZÁMER

Povinná osoba	Mesto Ružomberok
Názov projektu	Podpora v oblasti kybernetickej a informačnej bezpečnosti v meste Ružomberok
Zodpovedná osoba za projekt	PhDr. Vladimíra Pazderová, PhD., projektový manažér
Realizátor projektu	Mesto Ružomberok
Vlastník projektu	Mesto Ružomberok

Schvaľovanie dokumentu

Položka	**Meno a priezvisko**	**Organizácia**	**Pracovná pozícia**	**Dátum**	**Podpis** (alebo elektronický súhlas)
Vypracoval	PhDr. Vladimíra Pazderová, PhD.	Novo Funding s.r.o.	Projektový manažér	21.6.2024	
Schválil /za mesto/	Ing. Martin Žabenský	Mesto Ružomberok	Vedúci oddelenia IT	21.6.2024	

1. HISTÓRIA DOKUMENTU

Verzia	**Dátum**	**Zmeny**	**Meno**
1.0	14.6.2024	Prvá verzia dokumentu	PhDr. Vladimíra Pazderová, PhD.
1.1	21.6.2024	Finálna verzia dokumentu	PhDr. Vladimíra Pazderová, PhD.

2. ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE

V súlade s Vyhláškou č. 401/2023 Z.z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy je dokument Projektový zámer pre prípravnú a iniciačnú fázu určený na rozpracovanie detailných informácií prípravy projektu Podpora v oblasti kybernetickej a informačnej bezpečnosti v meste Ružomberok financovaného z výzvy č. PSK-MIRRI-611-2024-DV-EFRR.

2.1 Použité skratky a pojmy

SKRATKA/POJEM	**POPIS**
KIB	Kybernetická a informačná bezpečnosť
SIEM	Security Information and Event Management
SOC	Security Operations Center
IS	Informačný systém
SLA	Service Desk Manager
SW	Softvér
MsÚ	Mestský úrad
ISVS	Informačný systém verejnej správy
MCA	Multikriteriálna analýza
PZS	Poskytovateľ základnej služby

2.2 Konvencie pre typy požiadaviek (príklady)

3. DEFINOVANIE PROJEKTU

3.1 Manažérske zhrnutie

Pre oblasť kybernetickej a informačnej bezpečnosti v súčasnosti platí, že situácia, zabezpečenie a prijaté opatrenia nie sú dostatočné. Subjekty čoraz viac evidujú zvyšujúcu sa frekvenciu a závažnosť útokov, z interného hľadiska sa neustále zvyšuje závislosť na informačných aktívach a IT systémoch. Zvyšujú sa teda hrozby, zraniteľnosti a následne aj dopady bezpečnostných incidentov, ktoré evidujú aj subjekty v oblasti verejnej správy.

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe, ktoré nastavujú požiadavky a štandard z pohľadu bezpečnostných opatrení, sú povinné aj pre mestá ako poskytovateľov základných služieb, v dôsledku čoho sa mesto rozhodlo zapojiť sa do danej výzvy.

V sektore verejná správa, kde sa nachádza najväčší počet poskytovateľov základných služieb sa situácia v oblasti kybernetickej bezpečnosti dlhodobo nemení (Správa o kybernetickej bezpečnosti v Slovenskej republike v roku 2022). V tejto oblasti je možné pozorovať až kritické zanedbávanie bezpečnosti. Najmä samosprávy a menší prevádzkovatelia si dostatočne neuvedomujú dôležitosť témy kybernetickej bezpečnosti, k problematike pristupujú povrchovo a zameriavajú sa skôr na formálne aktivity, ako napríklad kupovanie generickej dokumentácie. Celkové riadenie kybernetickej bezpečnosti pri PZS v tomto sektore často chýba, je chaotické alebo čiastkové. Samosprávy sa snažia preniesť zodpovednosti pre túto oblasť na externých poskytovateľov služieb (podľa správy NBÚ, 2022).

Podľa štatistík Národného bezpečnostného úradu za rok 2022 /aktuálnejšie štatistiky nie sú dostupné/ je v sektore verejná správa 1417 poskytovateľov základných služieb, pričom počet PZS s povinnosťou auditu bol 1416 (bolo možné splniť aj samohodnotením podľa §34a ods. 2 ZoKB). Za rok 2022 bolo odovzdaných 99 auditných správ a 405 samohodnotení. Z odovzdaných auditov boli identifikované nasledovné nedostatky:

- nepreukázaný systém riadenia kybernetickej bezpečnosti,
- bezpečnostná stratégia kybernetickej bezpečnosti ani ďalšia bezpečnostná dokumentácia nebola predložená,
- manažér kybernetickej bezpečnosti nie je formálne menovaný, je v konfliktom záujmov a má nevhodne kumulované zodpovednosti,
- analýza rizík nie je zakotvená ako proces v interných predpisoch ani metodicky popísaná, nevykonáva sa,
- v organizácii sa nachádzajú vysoko privilegované účty, ktoré sú spoločné a nemajú definovaných vlastníkov a účel,
- v organizácii neexistuje definícia závažného kybernetického bezpečnostného incidentu, organizácia nevypracovala postupy a nemá dostatočné schopnosti na detekciu, zvládanie a poučenie sa z prípadných incidentov.

Uvedené nedostatky sú identifikované aj v meste Ružomberok. Mesto má pozíciu manažéra kybernetickej bezpečnosti obsadené externou osobou, prostredníctvom poskytovateľa tejto služby.

Vykonaný audit kybernetickej bezpečnosti z 12/2023 identifikoval viaceré nedostatky a nesúlad s legislatívou /26 identifikovaných nesúladov, 11 čiastkových súladov a 61 súladov/. Pri realizácii auditu kybernetickej bezpečnosti boli identifikované nasledovné závažné zistenia a nedostatky v jednotlivých oblastiach:

- zamestnanci pri ukončení pracovného pomeru alebo iného obdobného pracovného vzťahu zadoumentovaným spôsobom nevracajú späť všetky zverené aktíva
- identifikácia zraniteľnosti rizík je neaktualizovaná /posledná aktualizácia je z roku 2021/,
- identifikácia hrozieb sa nerobila, je zastaraná a nezodpovedá aktuálnemu zoznamu identifikovaných aktív,
- identifikácia a analýza rizík sa nerobila,
- dokumentácia KIB neobsahuje učeného vlastníka rizika,
- v meste nie sú zadefinované postupy pre presun práv a povinnosti k vzťahu ku kybernetickej bezpečnosti pre IT špecialistov a členov HT,
- PZS nemá vypracovaný plán vzdelávania, v rámci rozvoja bezpečnostného povedomia sa za posledné dva roky nekonalo žiadne školenie zamestnancov,
- nevykonáva sa kontrola dodržiavania bezpečnostných politík pre dodávateľov a zamestnancov,
- hodnotenie účinnosti plánu rozvoja bezpečnostného povedomia sa za posledné dva roky nerobilo,
- nie sú vypracované postupy pri skončení pracovného pomeru,
- PZS má identifikované tretie strany a s nimi uzavreté zmluvy, voči tretím stranám neboli vykonávané riziká spojené s dodávateľskými službami,
- vyhodnocovanie prevádzkových záznamov sa nevykonáva,
- nevykonáva sa detegovanie existujúcich zraniteľností programových prostriedkov a ich častí,
- PZS nepoužíva nástroj na detegovanie zraniteľnosti technických prostriedkov a ich častí,
- PZS nemá zavedený proces riadenia záplat a aktualizácií,
- bezpečnostná segmentácia siete nie je vytvorená,
- SIEM nie je vybudovaný,

- PZS nepoužíva nástroj na detekciu kybernetických bezpečnostných incidentov,
- nie je implementovaný nástroj na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí,
- zatiaľ nebola spracovaná analýza finančných nákladov na spracovanie dokumentácie BCM, technických a personálnych zdrojov,
- chýba BIA a RPO,
- neboli zatiaľ spracované procesy riadenia kontinuity činností a realizácie opatrení na zvýšenie odolnosti sietí a informačných systémov základnej služby.

Projekt "Podpora v oblasti kybernetickej a informačnej bezpečnosti v meste Ružomberok" je zameraný na posilnenie kybernetickej odolnosti a ochrany dát mesta a jeho obyvateľov. Cieľom projektu je realizovanie a financovanie opatrení KIB definované najmä v zákonoch č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a č. 95/2019 Z.z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov prostredníctvom modernizácie a optimalizácie súčasných procesov a technológií v oblasti informačných technológií a kybernetickej bezpečnosti, ako aj implementácia kritických bezpečnostných opatrení.

Projekt sa primárne sústredí na oblasti, kde mesto Ružomberok identifikovalo najvyššiu mieru rizika a najvyššie dopady, ako aj na oblasti, kde bola identifikovaná najvyššia miera nesúladu s legislatívnymi požiadavkami, vyplývajúce zo auditu kybernetickej bezpečnosti a z vykonanej analýzy rizík.

Realizácia projektu prispeje k naplneniu špecifických cieľov výzvy:

- ***RSO 1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy*** v rámci opatrenia 1.2.1 Podpora v oblasti informatizácie a digitálnej transformácie (oblasť - Kybernetická a informačná bezpečnosť)

Projekt je reakciou na narastajúce kybernetické hrozby a legislatívne požiadavky v oblasti ochrany dát a informačnej bezpečnosti. Jeho cieľom je zvýšiť odolnosť mesta proti kybernetickým útokom a zabezpečiť kontinuitu základných služieb prostredníctvom realizovanej hlavnej aktivity projektu - **Podpora v oblasti kybernetickej a informačnej bezpečnosti v meste Ružomberok,** v rámci ktorej sa budú realizovať nasledovné opatrenia:

1. **Aktualizácia analýzy rizík** zabezpečí správu aktív, zraniteľností, hrozieb a opatrení. Analýza rizík umožní aktualizovanie a hodnotenie rizík založené na aktuálnych dátach a poskytne nástroje pre efektívne riadenie a minimalizáciu rizík.
2. **Vybudovanie Security Incident and Event Management (SIEM):** Opatrenie je zamerané na vytvorenie nástroja zabezpečujúceho analýzu informácií zo všetkých sieťových zariadení, OS, databáz, aplikácií a pod., ktorými žiadateľ disponuje (SIEM), ktoré bude kompletne vybudované vo vlastníctve žiadateľa, tzv. on premise.
3. **Vypracovanie a implementácia komplexného plánu kontinuity činností (BCM),** ktorý zahŕňa postupy pre rýchlu obnovu kritických systémov a služieb po narušení. Plán bude obsahovať scenáre pre rôzne typy udalostí a zahrnie analýzu funkčných dopadov, strategické zdroje na obnovu a časové rámce pre reakciu.
4. **Modernizácia sieťovej infraštruktúry v mestskej informačnej sieti:** Zabezpečí sa výmena zastaraných sieťových prvkov, dobudovanie záložných trás a rozšírená segmentácia siete. Tieto kroky významne prispejú k zníženiu zraniteľností vyplývajúcich z používania EOL zariadení a ich nedostatočného zabezpečenia.
5. **Modernizácia serverovej infraštruktúry:** Výmena serverových komponentov, sieťových prvkov prispeje k zníženiu rizika nízkej dostupnosti poskytovania základnej služby a zraniteľnosti spojenej s používaním zastaraných zariadení.
6. **Zavedenie a správa nástroja na riadenie kapacít,** ktorý umožní nepretržité sledovanie všetkých IT aktív, poskytovanie včasných upozornení na potenciálne problémy a umožní rýchlu reakciu na incidenty. Týmto spôsobom sa zlepší viditeľnosť a kontrolu nad IT infraštruktúrou, čím sa zabezpečí jej spoľahlivú a bezpečnú prevádzku.
7. **Nastavenie zálohovania:** zavedenie stratégie a plánov zálohovania zabezpečí zvýšenie dostupnosti základnej služby.
8. **Implementácia next-gen firewall technológie:** Umožní pokročilé filtrovanie obsahu, riadenie prestupov medzi sieťovými segmentami a integráciu s aktuálnymi bezpečnostnými systémami. Táto technológia adresuje zraniteľnosti spojené s nedostatočnou kontrolou sieťového obsahu a potenciálnymi sieťovými útokmi na infraštruktúru
9. **Vykonanie auditu kybernetickej bezpečnosti:** Vykonanie auditov a penetračných testov na konci projektu poskytne hodnotné prehľady o efektívnosti prijatých opatrení a pomôže identifikovať ďalšie možnosti zlepšenia.

Tieto kroky sú navrhnuté tak, aby poskytli komplexný pohľad na bezpečnostný stav mesta a umožnili rýchlu a efektívnu reakciu na potenciálne incidenty, zabezpečila sa lepšia izolácia a ochranu rôznych častí mestskej siete.

Realizáciou projektu bude zabezpečené naplnenie nasledujúcich merateľných ukazovateľov:

1. ukazovatele výstupu:

- PO095 / PSKPSOI12 - *Verejné inštitúcie podporované v rozvoji kybernetických služieb, produktov a procesov* - ***1 verejná inštitúcia - Mesto Ružomberok*** */možné overiť v* štatistickom registri organizácií vedenom Štatistickým úradom SR, ktoré sú zaradené v sektore verejnej správy/

2. ukazovatele výsledku:

- PR017 / PSKPRCR11 - *Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov* - ***276 používateľov*** /103 interní zamestnanci mesta + 29 zamestnancov Mestskej polície + 144 zamestnancov materských a základných škôl /používatelia IKT Mesta Ružomberok/.

Celkový rozpočet projektu je stanovený na 593 188,58 Eur, pričom finančné prostriedky sú určené na krytie nákladov spojených s vývojom, nákupom, implementáciou riešení pre oblasť kybernetickej a informačnej bezpečnosti.

Hlavným prínosom projektu bude zvýšenie úrovne KIB, zníženie rizika incidentov, zlepšená spokojnosť a dôvera používateľov v digitálne služby mesta a posilnené povedomia zamestnancov o dôležitosti prijatých bezpečnostných opatrení.

Projekt je naplánovaný na obdobie od januára 2025, s očakávaným dokončením v decembri 2025, aby sa zaistila jeho účinnosť a prispôsobenie sa rýchlo meniacemu kybernetickému prostrediu. Tento projekt predstavuje kritický krok pre mesto v zabezpečení jeho digitálnej infraštruktúry a ochrane pred kybernetickými hrozbami, čo prispieva k bezpečnejšiemu a odolnejšiemu prostrediu pre všetkých jeho obyvateľov a návštevníkov.

Projekt je predkladaný v rámci výzvy *PSK-MIRRI-611-2024-DV-EFRR Podpora v oblasti kybernetickej a informačnej bezpečnosti na regionálnej úrovni - verejná správa.* Projekt bude implementovaný v rámci Programu Slovensko a jeho špecifického cieľa RSO 1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy, v rámci Opatrenia 1.2.1 Podpora v oblasti informatizácie a digitálnej transformácie (Oblasť - Kybernetická a informačná bezpečnosť).

3.2 Motivácia a rozsah projektu

Mesto Ružomberok stojí pred výzvami v oblasti kybernetickej a informačnej bezpečnosti, ktoré sú dôsledkom narastajúcich kybernetických hrozieb a stále prísnejších legislatívnych požiadaviek na ochranu dát poskytovateľov základných služieb. Súčasná úroveň kybernetickej a informačnej bezpečnosti nie je adekvátne pripravená na odvrátenie týchto hrozieb, čo ohrozuje nielen bezpečnosť dát občanov, ale aj celkovú integritu mestských informačných systémov a infraštruktúry.

Mesto Ružomberok, ako poskytovateľ základnej služby má vypracovanú bezpečnostnú stratégiu kybernetickej bezpečnosti a zadefinované bezpečnostné politiky pre riadenie informačnej bezpečnosti. Jedná sa o dokumenty obsahujúce súbor štandardov, postupov, zodpovedností a povinností, ktorých dodržiavanie a plnenie vytvára základný predpoklad k dosiahnutiu stanovených cieľov bezpečnostnej politiky pre riadenie informačnej bezpečnosti v meste. Bezpečnostná dokumentácia v meste Ružomberok však nebola schválená a implementovaná do praxe. Mesto ako poskytovateľ základnej služby má ustanovenú pozíciu manažéra kybernetickej bezpečnosti.

Celková úroveň riadenia kybernetickej bezpečnosti v zmysle požiadaviek zákona č. 69/2018 Z.z., vyhlášky 362/2018 Z.z. a zavedených opatrení je v meste Ružomberok čiastočne splnená /hodnotenie v rámci auditu kybernetickej bezpečnosti/. PZS vykonáva procesy na základe schválenej a vydanej dokumentácie, v zmysle požiadaviek Vyhlášky č. 362/2018 Z. z. Vyhláška Národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. Stratégia kybernetickej bezpečnosti mesta obsahuje všetky požadované náležitosti definované v prílohe č. 1 k vyhláške č. 362/2018 Z. z.

Zavedený proces klasifikácie informácií v meste Ružomberok je v súlade s požiadavkami vyhlášky č. 362/2018 Z. z. pre klasifikáciu informácií kategorizácia sietí a informačných systémov. Silnými stránkami plnenia opatrení kybernetickej bezpečnosti je vypracovaná dokumentácia ku kybernetickej bezpečnosti s prepojením na základnú službu.

Veľký priestor na zlepšenie oblasti kybernetickej bezpečnosti je hlavne v oblasti riadenia dodávateľov, plánovania vzdelávania osôb zastávajúce niektorú z bezpečnostných rolí, a v dopracovaní existujúcej bezpečnostnej dokumentácie kybernetickej bezpečnosti o interné dokumenty a smernice, ktoré nie sú v nej zapracované a doplnení identifikovaných zistení pri audite. Slabou stránkou riadenia kybernetickej bezpečnosti je detekcia bezpečnostných incidentov, postupov reakcie pri kybernetických útokoch. Nie je zavedený systém pre zber a analýzu bezpečnostných udalostí vytváraných IT prostriedkami v reálnom čase (SIEM). V oblasti riadenia rizík chýba nástroj, ktorým by sa efektívne preskúmavali a aktualizovali identifikované riziká v závislosti od prijatých bezpečnostných opatrení.

Veľkú pozornosť treba venovať aj aktualizácii operačných systémov. Na serveroch s nainštalovaným operačným systémom MS Windows server 2012 R2 je potrebné bezodkladne vykonať aktualizáciu operačného systému resp. vymeniť starý server za nový, ak daný HW už neumožňuje aktualizáciu OS. Operačný systém, ktorý už nie je podporovaný výrobcom môže mať za následok vzniku vážneho bezpečnostného incidentu.

V prípade kybernetického bezpečnostného útoku alebo vzniknutého incidentu neexistujú postupy pre obnovu napadnutých systémov. Tieto postupy a opatrenia musia byť rozpísané v kontinuite riadenia kybernetickej bezpečnosti (BCM). Nevyhnutným predpokladom efektívneho plánovania kontinuity je, aby boli vopred definované scenáre rôznych udalostí, ktoré potencionálne môžu mať negatívny vplyv na bežné činnosti organizácie. Nie sú zadefinované časy obnovy pre každú udalosť, ktorá by mohla nastať. Plánovanie kontinuity organizácie stanoví požiadavky na zdroje (adekvátnych finančných, materiálno-technických a personálnych zdrojov), ktoré budú potrebné na implementáciu vybraných stratégií kontinuity činností. Nevyhnutnou požiadavkou je aj obsadiť pracovné role, ktoré sú nevyhnutné pre plánovanie a riadenie kontinuity. Tieto požiadavky treba zaviesť v čo najkratšom čase.

Po odstránení nezhôd má organizácia - mesto Ružomberok vysoký potenciál v relatívne krátkom čase dosiahnuť primeranú úroveň kybernetickej bezpečnosti na dosiahnutie bezpečnej a spoľahlivej prevádzky základnej služby.

Kontrola súladu v zmysle normy STN ISO/IEC 27001 vykonaná manažérom kybernetickej bezpečnosti poukázala na jednotlivé oblasti nesúladu:

- **aspekty informačnej bezpečnosti v riadení kontinuity** /0%/ - organizácia by mala určiť svoje požiadavky na informačnú bezpečnosť a kontinuitu riadenia informačnej bezpečnosti v nepriaznivých situáciách, napr. počas krízy alebo

katastrofy. Organizácia by mala overiť vytvorené a zavedené opatrenia na kontinuitu informačnej bezpečnosti v pravidelných intervaloch, aby sa zabezpečila ich platnosť a efektívna funkčnosť počas nepriaznivých situácií.

- **riadenie vzťahov s dodávateľmi** /15,31%/ - potrebné zabezpečiť ochranu aktív organizácie, ku ktorým pristupujú dodávatelia. Požiadavky informačnej bezpečnosti na zníženie rizík spojených s dodávateľskými prístupmi do aktív organizácie by mali byť odsúhlasené s dodávateľom a formálne zdokumentované. Mali by byť definované všetky relevantné požiadavky informačnej bezpečnosti a odsúhlasené s každým dodávateľom, ktorý môže mať prístup k informáciám organizácie, spracúvať ich, ukladať, komunikovať alebo poskytovať infraštruktúrne komponenty.
- **riadenie aktív** /19,44%/ - potrebné identifikovať aktíva organizácie a definovať zodpovednosť za primeranú ochranu. Aktíva prepojené s informáciami a zariadeniami, ktoré informácie spracúvajú, mali by byť označené a mal by sa vytvoriť ich zoznam, ktorý by sa mal udržiavať. Aktíva udržiavané v inventári by mali mať vlastníka. Pravidlá na prijateľné používanie informácií a aktív spojených s prostriedkami na spracúvanie informácií by mali byť identifikované, zdokumentované a implementované.
- **šifrovanie a kryptografia** /20%/ - potrebné zabezpečiť správne a efektívne používanie kryptografie na zabezpečneie dôvernosti, preukázania pôvodu alebo integrity informácií. Na používanie kryptografických opatrení na ochranu informácií by mali byť vytvorené a zavedené politiky. Na zavedenie kryptografických opatrení je potrebná politika, aby sa maximalizoval účinok, aby sa minimalizovali riziká spojené s používaním metód šifrovania a zabránilo sa nevhodnému alebo nesprávnemu používaniu.
- **súlad** /29,63%/ - potrebné zabrániť vzniku právnych, štatutárnych, regulačných a zmluvných porušení povinností vo vzťahu
- organizácia informačnej bezpečnosti a akýmkoľvek bezpečnostným požiadavkám. Všetky relevantné štatutárne, regulačné a zmluvné požiadavky by mali byť explicitne definované, dokumentované a udržiavané v aktuálnej podobe pre každý informačný systém a organizáciu ako celok.
- **personálna bezpečnosť** /36,52%/ - potrebné zabezpečiť, že zamestnanci a zmluvní partneri rozumejú svojej zodpovednosti a že sú vhodní na výkon rolí, ktoré im boli pridelené. Mala by sa vykonať verifikačná previerka personálneho pozadia všetkých uchádzačov o zamestnanie v súlade s príslušnými zákonmi, právnymi nariadeniami a etikou, ako aj vzhľadom na obchodné požiadavky, klasifikačný stupeň informácií, ku ktorým sa bude pristupovať, ako aj na vnímané riziká.
- **komunikačná bezpečnosť** /48%/ - potrebné zabezpečiť ochranu v sieťach a v podporných zariadeniach, ktoré ich v sieťach spracúvajú. Siete by mali byť primerane riadené a spracované, čím a zabezpečí ochrana informácií v systémoch a aplikáciách.
- **bezpečnosť prevádzky** /51,2%/ - potrebné zabezpečiť správnu a bezpečnú prevádzku zariadení spracúvajúcich informácie.
- riadenie prístupov. Použite prostriedkov by sa malo monitorovať, dolaďovať a mali by sa robiť odhady budúcich požiadaviek na kapacity, čím sa zabezpečí dosiahnutia požadovanej výkonnosti systému. Pravidelne by sa mali robiť a testovať záložné kópie dôležitých informácií a softvéru v súlade so schválenou politikou zálohovania.
- **akvizícia, vývoj a údržba informačných systémov** /60,53%/ - požiadavky spojené s informačnou bezpečnosťou by mali byť začlenené do požiadaviek pre nové informačné systémy alebo do požiadaviek rozšírenia existujúcich informačných systémov. Implementácia zmien do systémov v rámci životného cyklu by mala byť riadená prostredníctvom formálnych procedúr riadenia zmien. Pri zmene operačného systému by sa mala vykonať revízia kritických aplikácií, ako aj testovanie s cieľom zabezpečiť, že to nebude mať za následok negatívny vplyv na prevádzku organizácie alebo na bezpečnosť.
- **fyzická bezpečnosť a bezpečnosť prostredia** /66,67%/ - potreba zabezpečiť neoprávnenému fyzickému prístupu, zničeniu alebo zasahovaniu do informácií organizácie alebo zariadení spracúvajúcich informácie.
- **riadenie incidentov informačnej bezpečnosti** /67,44%/ - potreba zabezpečiť konzistentný a efektívny prístup na riadenie incidentov informačnej bezpečnosti vrátane komunikácie o bezpečnostných udalostiach a slabinách. Mali by sa zaviesť

Stratégia kybernetickej bezpečnosti mesta Ružomberok z mája 2024 definuje nasledovné strategické ciele pre oblasť KIB:

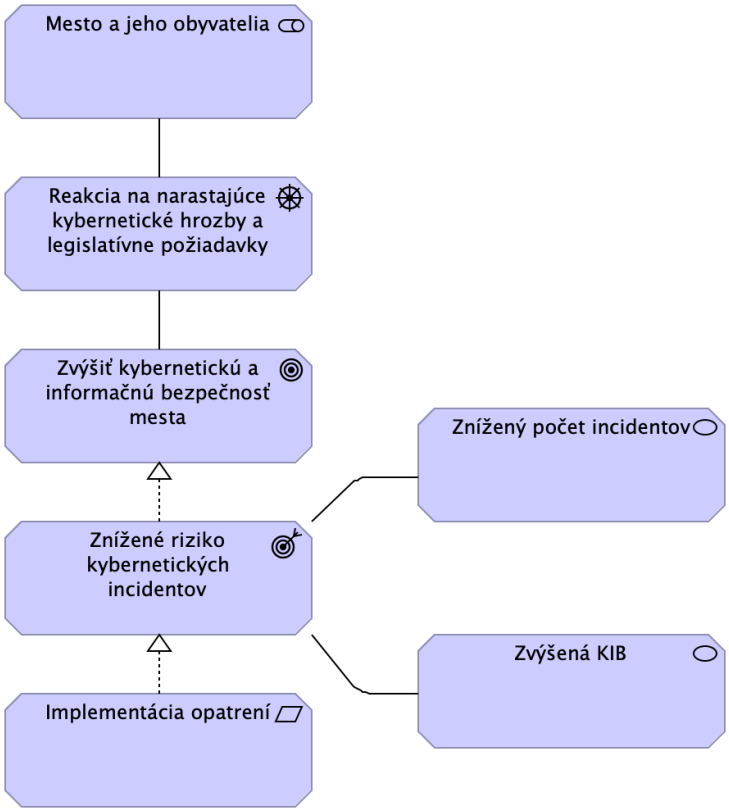
- Vybudovať a trvalo udržiavať vysokú úroveň ochrany, kybernetickej bezpečnosti a bezpečnosti informačných systémov.
- Vytvoriť podmienky a realizovať bezpečné rozmiestnenie najdôležitejších IKT komponentov a trvalo zabezpečovať ich technickú a režimovú ochranu.
- Obstarávať a implementovať informačné systémy len vysokej kvalitatívnej a odbornej úrovne a úžitkovej hodnoty.
- Uplatniť pri budovaní informačnej a kybernetickej bezpečnosti princíp vlastníctva.
- Chrániť práva občanov, zamestnancov a dodávateľov mesta.
- Zabezpečiť potrebnú ochranu majetku a objektov mesta.
- Zaviesť systém kontrol výkonu práce všetkých oddelení, útvarov i samotných zamestnancov s cieľom odhaliť nekvalitný, neprofesionálny alebo inak so záujmami mesta nezlučiteľný výkon práce.
- Zabrániť existujúcim formám obohacovania sa na úkor mesta.
- Vytvoriť a udržiavať havarijné plány pre všetky dôležité informačné systémy mesta.
- Vytvoriť a udržiavať funkčnú štruktúru, ktorá bude zabezpečovať dosiahnutie a udržanie stanovenej cieľovej úrovne informačnej a kybernetickej bezpečnosti vo všetkých požadovaných oblastiach.
- Zaviesť a trvalo zabezpečovať systém hlásení o stave bezpečnostného systému a hlásení o bezpečnostných a kybernetických incidentoch.
- Vykonávanie auditu zavedenia informačnej a kybernetickej bezpečnosti.

Projekt zasahuje do množstva biznis procesov mesta Ružomberok vrátane tých, ktoré sú zamerané na spracovanie a ochranu citlivých údajov, riadenie prístupu k informačným systémom, ako aj na efektívnu reakciu na potenciálne bezpečnostné incidenty. Cieľom je posilniť tieto procesy, čím sa zvýši odolnosť mesta voči kybernetickým hrozbám.

Projekt sa špecificky sústredí na zlepšenie v oblasti kybernetickej a informačnej bezpečnosti, ktorá je nevyhnutná pre zabezpečené a efektívne fungovanie mestskej správy a poskytovanie základných služieb obyvateľom. To zahŕňa implementáciu kľúčových bezpečnostných opatrení, ako sú napr. systémy SIEM ako aj zlepšenie infraštruktúry a procesov súvisiacich s bezpečnosťou sietí a dát.

Hlavnou motiváciou je zabezpečiť, aby mesto Ružomberok bolo schopné efektívne reagovať na kybernetické hrozby, ochraňovať dáta svojich obyvateľov a zabezpečiť neprerušené poskytovanie kritických služieb. Zároveň budú realizované opatrenia, ktoré boli identifikované v rámci Analýzy rizík /aktualizovaná v 2024/ a spracovaným auditom kybernetickej bezpečnosti /spracovaný v 2024/, ktoré pomôžu výrazne znížiť identifikované riziká v rámci jednotlivých opatrení.

Projekt čelí obmedzeniam, ako sú obmedzené finančné zdroje /vlastné zdroje mesta/, potreba zabezpečenia súladu s legislatívou a nevyhnutnosť spolupráce naprieč rôznymi oddeleniami Mestského úradu. Prekonanie týchto prekážok bude kľúčové pre úspešné dosiahnutie cieľov projektu a zabezpečenie dlhodobej udržateľnosti zvýšenej úrovne kybernetickej a informačnej bezpečnosti v meste Ružomberok.



Obrázok 1 Motivačná architektúra projektu

V rámci rozsahu projektu, Mesto Ružomberok sa rozhodlo zvoliť najefektívnejšie technologické riešenie, ktoré prispeje k eliminácii najkritickejších problémov v oblasti kybernetickej a informačnej bezpečnosti. V rámci hlavnej aktivity projektu sa budú realizovať nasledovné opatrenia:

Č.	Názov opatrenia	Popis	Výstup	Dopad/následok
1.	**Aktualizácia analýzy rizík**	Aktualizácia analýzy rizík zabezpečí správu aktív, zraniteľností, hrozieb a opatrení. Analýza rizík umožní aktualizovanie a hodnotenie rizík založené na aktuálnych dátach a poskytne nástroje pre efektívne riadenie a minimalizáciu rizík.	1. Aktualizácia analýzy rizík, hrozieb a zraniteľností, ktorej výsledky budú slúžiť ako východisko pre klasifikáciu informácií, kategorizáciu sietí a informačných systémov. 2. Aktualizácia klasifikácie informácií a kategorizácie sietí a informačných systémov, podľa klasifikačnej schémy v súlade s prílohou č.2 vyhlášky 362/2018.	*- zníženie zraniteľnosti vyplývajúcej s nedostatočného riadenie rizík a opatrení v oblasti KB*
2.	**Vybudovanie SIEM**	Monitorovanie hrozieb v reálnom čase prostredníctvom	1. Implementácia SIEM 2. Dokumentácia a školenie.	*- zníženie zraniteľnosti - zrýchlenie reakcie pri bezpečnostných incidentoch (okamžité upozornenia na*

		systémov ako SIEM, zabezpečí rýchlu reakciu na potenciálne bezpečnostné incidenty a výrazne prispieva k celkovej odolnosti mesta.		*neobvyklé udalosti)*
3.	**Vypracovanie a implementácia komplexného plánu kontinuity činností**	Vypracovanie a implementácia plánu kontinuity činností (BCM), ktorý zahŕňa postupy pre rýchlu obnovu kritických systémov a služieb po narušení. Plán bude obsahovať scenáre pre rôzne typy udalostí a zahrnie analýzu funkčných dopadov, strategické zdroje na obnovu a časové rámce pre reakciu.	1. Plán kontinuity činností musí obsahovať minimálne: a. Plán kontinuity na stanovenie požiadaviek a zdrojov b. Plán reakcie na incidenty a plány havarijnej obnovy prevádzky c. Politiku a ciele kontinuity d. Analýzu funkčných dopadov e. Stratégiu riadenia kontinuity vrátane evakuačných postupov f. Plán údržby a kontroly BCMS. 2. Školenie	*- zníženie zraniteľnosti - zrýchlenie reakcie pri bezpečnostných incidentoch (okamžité upozornenia na neobvyklé udalosti)*
4.	**Modernizácia sieťovej infraštruktúry v mestskej informačnej sieti**	Zabezpečí sa výmena zastaraných sieťových prvkov, dobudovanie záložných trás a rozšírená segmentácia siete. Tieto kroky významne prispejú k zníženiu zraniteľností vyplývajúcich z používania EOL zariadení a ich nedostatočného zabezpečenia.	1. Vstupná analýza existujúcej sieťovej infraštruktúry a návrhu opatrení v zmysle vyhlášky NBU č.362/2018. 2. Výmena a inštalácia zastaralých sieťových prvkov na úrovni L2/L3. 3. Rekonfigurácia siete vrátane rozšírenej segmentácie a rozdelenia na VLAN. 4. Vytvorenie alebo aktualizácia dokumentácie počítačovej siete, ktorá obsahuje evidenciu všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológiu siete a využitie IP rozsahov 5. Zaškolenie IT personálu	*- zníženie zraniteľnosti vyplývajúcej z použitia EOL zariadení (nedostatočné zabezpečenie)* *- zníženie zraniteľnosti vyplývajúcej nízkej dostupnosti poskytovania základnej služby.*
5.	**Modernizácia serverovej infraštruktúry**	Výmena serverových komponentov, sieťových prvkov prispeje k zníženiu rizika nízkej dostupnosti poskytovania základnej služby a zraniteľnosti spojenej s používaním zastaraných zariadení.	1. Výmena serverov. 2. Výmena sieťových prvkov pre iSCSI. 3. Nasadenie platformy pre beh VM 4. Kompletná konfigurácia, dokumentácia a , zaškolenie IT pracovníkov 5. Montáž, inštalácia serverov a storage a ich prepojenie, nastavenie Domény, konfigurácia Active Directory, migrácia dát a migrácia databáz. 6. Aktualizácia, vypracovanie a dodanie príslušnej systémovej a používateľskej dokumentácie k vykonaným zmenám 7. Zaškolenie IT personálu	*- zníženie zraniteľnosti vyplývajúcej z použitia EOL zariadení (nedostatočné zabezpečenie)* *- zníženie zraniteľnosti vyplývajúcej nízkej dostupnosti poskytovania základnej služby.*
6.	**Zavedenie a správa nástroja na riadenie kapacít**	Nástroj na riadenie kapacít umožní nepretržité sledovanie všetkých IT aktív, poskytovanie včasných upozornení na potenciálne problémy a umožní rýchlu reakciu na	1. Inštalácia a základná konfigurácia. 2. Nastavenie monitorovacích objektov. 3. Konfigurácia upozornení a eskalácií. 4. Vizuálne rozhrania a reporty 5. Integrácia a rozšírenia. 6. Bezpečnosť a prístupové práva. 7. Školenie a podpora.	*- zníženie zraniteľnosti - zrýchlenie reakcie pri bezpečnostných incidentoch (okamžité upozornenia na neobvyklé udalosti)*

		incidenty. Týmto spôsobom sa zlepší viditeľnosť a kontrolu nad IT infraštruktúrou, čím sa zabezpečí jej spoľahlivú a bezpečnú prevádzku.		
7.	**Nastavenie zálohovania**	Zavedenie stratégie a plánov zálohovania zabezpečí zvýšenie dostupnosti základnej služby.	1. Analýza a plánovanie zálohovania 2. Konfigurácia zálohovacieho softvéru 3. Automatizácia a monitorovanie. 4. Testovanie a validácia zálohovania 5. Školenie a dokumentácia	*- zníženie zraniteľnosti vyplývajúcej s potencionálnej straty údajov (zlyhanie HW, ransomware atd.)*
8.	**Dodanie a implementácia next-gen firewall technológie**	Umožní pokročilé filtrovanie obsahu, riadenie prestupov medzi sieťovými segmentami a integráciu s aktuálnymi bezpečnostnými systémami	Dodanie a implementácia next-gen firewall technológie vrátane: 1. Analýza súčasného stavu 2. Návrh implementačného konceptu a dizajnu riešenia 3. Inštalácia nového HW v priestoroch objednávateľa 4. Základná konfigurácia FW (IP adresa, názov, zóny, manažment ....) 5. Vytváranie nových pravidiel podľa pripraveného konceptu 6. Konfigurácia VPN tunelov 7. Migrácia objektov, smerovania, NAT 8. Migrácia komunikačných pravidiel 9. Integrácia so všetkými prvkami sieťovej infraštruktúry 10. Testovanie riešenia v testovacom prostredí 11. Migrácia do produkčného prostredia 12. Vyriešenie komunikačných problémov (prepojenie na externé subjekty, portály a pod. 13. Z inštalácie a kompletnej konfigurácie zariadenia 14. Aktualizácia, vypracovanie a dodanie príslušnej systémovej a používateľskej dokumentácie k vykonaným zmenám 15. Zaškolenie IT personálu	– *zníženie zraniteľnosti vyplývajúcej z nedostatočnej kontroly obsahu, monitorovania a analýzy informácií (únik informácií z vnútra, bezpečnostné incidenty)* – *zníženie zraniteľnosti vyplývajúcej z potencionálnych sieťových útokov na infraštruktúru MsÚ (DDoS, password attack, spoofing, neautorizovaný prístup..)*
9.	**Vykonanie auditu kybernetickej bezpečnosti**	Vykonanie auditu a na začiatku a na konci projektu poskytne hodnotný prehľad o efektívnosti prijatých opatrení a pomôže identifikovať ďalšie možnosti zlepšenia.	1. Audit kybernetickej bezpečnosti v zmysle platného zákona o kybernetickej bezpečnosti. a. Vykonaný audit b. Záverečná správa o výsledkoch vykonaného auditu	*- vyhodnotenie dopadu prijatých opatrení na zvýšenie kybernetickej bezpečnosti*

Tabuľka 1 Obsah projektu

Implementáciou týchto opatrení bude dosiahnuté výrazné zvýšenie odolnosti prevádzky siete voči kybernetickým útokom, výrazné zvýšenie bezpečnosti prevádzky, zväčšenie dostupnosti služieb Mesta Ružomberok. Projekt umožní vytvoriť robustnejšiu infraštruktúru, ktorá bude funkčne a kapacitne vyhovovať potrebám nevyhnutným pre poskytovanie služieb Mesta Ružomberok a z bezpečnostného hľadiska spĺňať legislatívne požiadavky. Zároveň projekt umožní nastaviť procesy a postupy, ako tento stav v čase zachovať a rozvíjať v nadväznosti na požiadavky vyplývajúce zo zmeny legislatívy, resp. rozsahu poskytovaných služieb.

3.3 Zainteresované strany/Stakeholderi

V rámci projektu "Podpora v oblasti kybernetickej a informačnej bezpečnosti v meste Ružomberok" sú zainteresované rôzne strany, ktoré zohrávajú kľúčovú úlohu v jeho realizácii a budúcom fungovaní. Tieto strany zastávajú rozličné role, od rozhodovania a riadenia projektu až po jeho konkrétnu implementáciu a využívanie výsledkov. Tu je prehľad hlavných zainteresovaných strán a ich rolí v projekte:

ID	AKTÉR / STAKEHOLDER	SUBJEKT (názov / skratka)	ROLA (vlastník procesu/ vlastník dát/zákazník/ užívateľ …. člen tímu atď.)	Informačný systém (MetaIS kód a názov ISVS)
1.	*Mestský úrad Ružomberok*	*Mesto Ružomberok*	Vlastník a implementátor procesu	ISVS poskytujúce základné služby
2.	*Interní zamestnanci Mesta Ružomberok*	*Mesto Ružomberok*	Používateľ	
3.	*Manažér kybernetickej bezpečnosti*	*Mesto Ružomberok*	Zodpovednosť za oblasť KIB Mesta Ružomberok	
4.	*Vybrané mestské organizácie*	*Mesto Ružomberok*	Používateľ	
5.	*Občan / podnikateľ*		Používateľ	
6.	*Poskytovateľ IT služby*		Poskytovateľ alebo konzument údajov IS Mesta Ružomberok v podobe dátových zdrojov otvorených dát alebo vo forme služieb resp. rozhraní	

Tabuľka 2 Stakeholderi projektu

3.4 Ciele projektu

Ciele projektu sú definované v súlade s Národnou koncepciou informatizácie verejnej správy a očakávanými výsledkami definovaných v Partnerskej dohode SR na roky 2021-2027. Definície tiež vychádzajú z národnej stratégie kybernetickej bezpečnosti na roky 2021 - 2025.

Hlavný cieľ projektu:

- ***realizovanie a financovanie opatrení KIB definované najmä v zákonoch č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a č. 95/2019 Z.z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov,*** *čo nadväzuje na RSO 1.2* ***Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy*** v rámci opatrenia 1.2.1 Podpora v oblasti informatizácie a digitálnej transformácie (oblasť - Kybernetická a informačná bezpečnosť)

Čiastkové ciele projektu:

- ***Modernizácia sieťovej infraštruktúry*** */v rámci oprávnenej podaktivity i) Sieťová a komunikačná bezpečnosť v rámci Výzvy/,*
- ***Zabezpečenia zálohovacích riešení*** */v rámci oprávnenej podaktivity n) Kontinuita prevádzky/,*
- ***Zabezpečenie riadenia a dodržiavania opatrení kybernetickej bezpečnosti*** */v rámci oprávnenej podaktivity b) Riadenie rizík a v súlade s ďalšími opatreniami v rámci spracovania dokumentácie/,*
- ***Zaistenie bezpečnosti pri prevádzke informačných systémov a sietí*** */v rámci oprávnenej podaktivity f) Bezpečnosť pri prevádzke informačných systémov a sietí/,*
- ***Zaznamenávanie udalostí a monitorovanie a riešenie KIB incidentov*** */v rámci oprávnenej podaktivity k) Zaznamenávanie udalostí a monitorovanie v rámci Výzvy/,*
- ***Zabezpečenie kontinuity prevádzky*** */v rámci oprávnenej podaktivity n) Kontinuita prevádzky/*
- ***Zabezpečenie auditu a kontrolných činností*** */v rámci oprávnenej podaktivity o) Audit a kontrolné činnosti/.*

Súlad cieľov v rámci relevantných strategických dokumentov v oblasti KIB:

ID	Názov cieľa	Názov strategického cieľa	Spôsob realizácie strategického cieľa
1.	Program Slovensko - Opatrenia 1.2.1 Podpora v oblasti informatizácie a digitálnej transformácie (oblasť -	RSO 1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány	Rozvoj a implementácia konkrétnych technologických a organizačných opatrení, ktoré sú zamerané na posilnenie

	Kybernetická a informačná bezpečnosť)	verejnej správy	kybernetickej odolnosti a zabezpečenie dát mesta a jeho obyvateľov.
2.	NKIVS - Strategická priorita Kybernetická a informačná bezpečnosť	Zvýšenie schopnosti včasnej identifikácie kybernetických incidentov vo verejnej správe	Projekt zvýši mestu schopnosť včasnej identifikácie kybernetických incidentov prostredníctvom implementácie systému SIEM pre real-time analýzu a monitorovanie bezpečnostných udalostí.
3.	Národná stratégia kybernetickej bezpečnosti - Strategický ciel Kybernetická bezpečnosť ako základná súčasť verejnej správy	Kybernetická bezpečnosť ako základná súčasť verejnej správy	Výsledkom projektu bude zvýšenie ochrany prevádzkovateľa základných služieb mesta z hľadiska kybernetickej bezpečnosti. Toto bude preukázané aj auditom na konci projektu ktorý preukáže pozitívny trend zlepšovania stavu kybernetickej bezpečnosti v meste.

Tabuľka 3 Ciele projektu

3.5 Merateľné ukazovatele (KPI)

ID	ID/Názov cieľa	Názov ukazovateľa (KPI)	Popis ukazovateľa	Merná jednotka	AS IS merateľné hodnoty (aktuálne)	TO BE Merateľné hodnoty (cieľové hodnoty)	Spôsob ich merania	Pozn.
1	PO095 / PSKPSOI12	Verejné inštitúcie podporované v rozvoji kybernetických služieb, produktov a procesov	Počet verejných inštitúcií, ktoré sú podporované za účelom rozvoja a modernizácie kybernetických služieb, produktov, procesov a zvyšovania vedomostnej úrovne napríklad v kontexte opatrení smerujúcich k elektronickej bezpečnosti verejnej správy.	verejné inštitúcie	0	**1 verejná inštitúcia -** Mesto Ružomberok	Identifikácia počtu realizácie opatrení KIB pre inštitúciu – splnenie súladu KIB so zákonom o kybernetickej bezpečnosti a zákonom o ISVS Čas plnenia merateľného ukazovateľa projektu: Fyzické ukončenie realizácie hlavných aktivít projektu	Typ ukazovateľa: Výstup
2	PR017 / PSKPRCR11	Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov	Počet používateľov nových vylepšených verejných digitálnych služieb, produktov a procesov	Používatelia/rok	0	**276 používateľov -** /103 interní zamestnanci mesta + 29 zamestnancov Mestskej polície + 144 zamestnanci materských a základných škôl /používatelia IKT Mesta Ružomberok/	Sumarizácia počtu používateľov nových a vylepšených digitálnych služieb – bude určené počtom prístupov v IAM, Databázou používateľov v oblasti KIB. V prípade Mesta Ružomberok ide o počet zamestnancov, ktorí využívajú IS Mesta alebo akékoľvek elektronické zariadenia v správe mesta. Čas plnenia merateľného ukazovateľa projektu: v rámci udržateľnosti projektu	Typ ukazovateľa: Výsledok

Tabuľka 4 Merateľné ukazovatele projektu

3.6 Špecifikácia potrieb koncového používateľa

V kontexte Mesta Ružomberok, koncovým používateľom je IT oddelenie a sekundárne tiež interní zamestnanci Mesta Ružomberok, podnikateľské subjekty pôsobiace na území mesta, ktoré očakávajú, že nebude vplyvom kybernetických útokov dochádzať k výpadkom prevádzky informačných systémov mesta, ktoré by znefunkčnili poskytovanie základnej služby Mesta Ružomberok.

Z výsledkov kybernetického auditu vyplynuli definície potrieb a požiadaviek na realizáciu konkrétnych opatrení v oblasti kybernetickej a informačnej bezpečnosti, v ktorých Mesto Ružomberok ako PZS dosahuje najvyšší nesúlad v zmysle zákona o kybernetickej bezpečnosti, zákona o ISVS a vyhlášky 362/2018 Z.z. Požiadavky potrieb koncového používateľa úzko koreluje s definovanými oblasťami/opatreniami, ktoré sú riešené v rámci predkladaného projektu.

Realizáciou projektu budú očakávania a potreby koncového používateľa naplnené.

Technický popis riešenia s cieľom zabezpečenia potrieb používateľa:

Opatrenie 1 - **Analýza rizík v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§6) v rovine riadenia, revízie a aktualizácie potrebnej dokumentácie**

Analýza rizík pozostáva z:

1. Aktualizácie analýzy rizík, hrozieb a zraniteľností,
2. Aktualizácie klasifikácie informácií a kategorizácie sietí a informačných systémov, podľa klasifikačnej schémy v súlade s prílohou č.2 vyhlášky 362/2018

Opatrenie 2 - Zavedenie bezpečnostných a analytických systémov na monitorovanie hrozieb v reálnom čase

Jedná sa o vybudovanie Security Incident and Event Management (SIEM) a zabezpečenie SOC (Security Operations Center) as a service. Opatrenie bude spočívať vo vytvorení nástroja zabezpečujúceho analýzu informácií zo všetkých sieťových zariadení, OS, databáz, aplikácií a pod. Vybudovaný SIEM bude tvoriť základ pre prevádzku Security Operation Center (SOC), ktorý bude zabezpečovať dohľad bezpečnosti sieťových zariadení, serverov, aplikácií a jednotlivých klientov. Vybudovaný SIEM bude zabezpečovať aktívny zber dát z monitorovaných zariadení a aplikácií v reálnom čase a následne zabezpečovať odhaľovanie potenciálnych hrozieb prostredníctvom automatizovanej korelácie dát zo zariadení. Priebežná analýza okamžite upozorní na neštandardné správanie systému, ktoré by mohlo predstavovať potenciálnu hrozbu. Odborná kapacita zabezpečujúca dohľad nad SOC-om takéto riziko vyhodnotí a určí či je hrozba kritická, alebo postačuje jej evidencia. Mesto plánuje vybudovanie kompletného hardvérového a softvérového riešenia SIEM v rámci svojho majetku a následnú prevádzku SOC plánuje zabezpečovať prostredníctvom služby u externého dodávateľa. Vytvorené riešenie umožní tiež zaviesť postup na využitie verejných a výrobcami poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

Opatrenie 3 - **Vypracovanie kontinuity činností v zmysle ZoKB – riadenie kontinuity činností (BCM) v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§17)**

Kontinuita činností musí zadefinovať scenáre rôznych udalostí, ktoré potenciálne môžu mať negatívny vplyv na bežné činnosti organizácie ako sú napríklad:

- náhla nedostupnosť personálu či nepoužiteľnosť pracoviska/budovy,
- nedostupnosť technologickej infraštruktúry či potrebných médií,
- incident či živelná katastrofa.

Súčasťou kontinuity činností bude vypracovanie analýzy funkčných dopadov a kvalifikácia potenciálnych dopadov a straty v prípade prerušenia alebo narušenia prevádzky u všetkých procesov organizácie. Kontinuitou budú zavedené postupy zálohovania na obnovy siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu

Opatrenie 4 - Návrh a segmentácia sieťovej infraštruktúry v informačnej sieti

Segmentácia sieťovej infraštruktúry bude pozostávať z:

1. Vstupnej analýzy existujúcej sieťovej infraštruktúry a návrhu opatrení v zmysle vyhlášky NBU č.362/2018,
2. Výmeny a inštalácie zastaralých sieťových prvkov na úrovni L2/L3,
3. Rekonfigurácie siete vrátane rozšírenej segmentácie a rozdelenia na VLAN,
4. Vytvorenie alebo aktualizácia dokumentácie počítačovej siete, ktorá obsahuje evidenciu všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológiu siete a využitie IP rozsahov,
5. Zaškolenie IT personálu.

Opatrenie 5 - Modernizácia serverovej infraštruktúry

Riešenie pozostáva z:

1. Výmeny serverov,
2. Výmeny sieťových prvkov pre iSCSI,
3. Nasadenia platformy pre beh VM,
4. Kompletnej konfigurácie, dokumentácie a zaškolenie IT pracovníkov
5. Montáže, inštalácie serverov a storage a ich prepojenie, nastavenia Domény, konfigurácie Active Directory, migrácie dát a migrácie databáz.
6. Aktualizácie, vypracovania a dodania príslušnej systémovej a používateľskej dokumentácie k vykonaným zmenám,
7. Zaškolenie IT personálu.

Opatrenie 6 - **Zavedenie a správa nástroja na riadenie kapacít v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§11) prostredníctvom systému na monitorovanie zariadení, technológií a služieb s dosahom na zabezpečenie kybernetickej bezpečnosti**

Riešením bude pokryté monitorovanie dostupných technologických kapacít dôležitých sieťových zariadení a služieb podľa nakonfigurovaných pravidiel. Monitorovací nástroj bude informovať o vzniknutých technických problémoch a nedostatku kapacít správcu príslušnej služby alebo servera a bude schopný monitorovať rôzne druhy zariadení ako sú fyzické a virtuálne servery, sieťové prvky, dátové úložiská a iné zariadenia, ktoré dokážu poskytnúť údaje o svojej prevádzke. Monitoring bude v reálnom čase údaje okamžite vizualizovať prostredníctvom grafov, máp a rôznych náhľadov a bude schopný porovnávať dáta v rôznych časových obdobiach, analyzovať históriu.

Opatrenie 7 - Nastavenie zálohovania

Riešenie pozostáva z:

- analýzy a plánovania zálohovania,
- konfigurácie zálohovacieho softvéru,
- automatizácie a monitorovania,
- testovanie a validácie zálohovania,
- školenia a dokumentácie.

Opatrenie 8 - Dodanie a implementácia next-gen firewall technológie
Riešenie umožní pokročilé filtrovanie obsahu, riadenie prestupov medzi sieťovými segmentami a integráciu s aktuálnymi bezpečnostnými systémami.

Opatrenie 9 - Vykonanie auditu kybernetickej bezpečnosti
Vykonanie auditu na konci projektu poskytne hodnotné prehľady o efektívnosti prijatých opatrení a pomôže identifikovať ďalšie možnosti zlepšenia. Dodávateľ vykoná Audit kybernetickej bezpečnosti v zmysle platného zákona o kybernetickej bezpečnosti, na ktorého konci poskytne Záverečná správu o výsledkoch vykonaného auditu.

3.7 Riziká a závislosti

Zoznam rizík a závislostí je uvedený v prílohe Zoznam rizík a závislosti.

3.8 Stanovenie alternatív v biznisovej vrstve architektúry

Alternatíva	Stručný popis	Výhody	Nevýhody
Alternatíva 1: Realizácia projektu v plnej miere	Kompletná realizácia všetkých naplánovaných opatrení na modernizáciu IT infraštruktúry a implementáciu bezpečnostných technológií, vrátane auditov. Cieľom je dosiahnuť maximálnu možnú úroveň kybernetickej a informačnej bezpečnosti a zabezpečiť celkovú odolnosť mesta proti kybernetickým hrozbám, ochranu citlivých dát a kontinuitu kritických služieb. Táto alternatíva predstavuje najkomplexnejšie riešenie, ktoré ponúka najvyššie zabezpečenie a zodpovedá aktuálnym a predpokladaným potrebám mesta.	1. Komplexné riešenie, ktoré adresuje všetky identifikované bezpečnostné hrozby a nedostatky. 2. Maximálna možná úroveň ochrany citlivých dát a IT infraštruktúry. 3. Zvýšenie odolnosti mesta proti kybernetickým útokom a zabezpečenie kontinuity kritických služieb. 4. Lepšia pripravenosť mesta vzhľadom na budúce technologické a bezpečnostné výzvy.	1. Potenciálne vysoké počiatočné náklady na implementáciu všetkých plánovaných opatrení. 2. Vyžaduje si rozsiahle zdroje a značné úsilie pri implementácii a školení zamestnancov.
Alternatíva 2: Čiastočná implementácia projektu	Realizácia len vybraných opatrení z celkového plánu, s dôrazom na najkritickejšie aspekty infraštruktúry a bezpečnosti. Takéto čiastočné riešenia by mohli zlepšiť súčasný stav, ale neponúkajú komplexné zabezpečenie a nezabezpečujú všetky identifikované potreby a riziká. Táto alternatíva by mohla viesť k nedostatočnej ochrane proti niektorým druhom hrozieb a k obmedzenej schopnosti reagovať na incidenty, čo by mohlo mať za následok vyššie dlhodobé náklady a riziká.	1. Riešenie, ktoré adresuje vybrané identifikované bezpečnostné hrozby a nedostatky. 2. Čiastočné zvýšenie úrovne ochrany citlivých dát a IT infraštruktúry. 3. Čiastočné zvýšenie odolnosti mesta proti kybernetickým útokom a zabezpečenie kontinuity kritických služieb. 4. Čiastočné zlepšenie pripravenosti mesta vzhľadom na budúce technologické a bezpečnostné výzvy.	1. Nezabezpečuje komplexnú ochranu pred všetkými potenciálnymi hrozbami. 2. Môže vytvárať bezpečnostné medzery v dôsledku neúplného pokrytia rizík. 3. Vyššie dlhodobé náklady a riziká v dôsledku potenciálne potrebných dodatočných zásahov.
Alternatíva 3: Udržiavanie súčasného stavu	Táto alternatíva predstavuje možnosť neuskutočniť žiadne zmeny a ponechať IT infraštruktúru a bezpečnostné opatrenia mesta v súčasnom stave. Tento prístup by znamenal výrazné riziká, keďže by sa neadresovali identifikované problémy a nedostatky v kybernetickej a informačnej bezpečnosti. Udržiavanie súčasného stavu by mohlo viesť k vážnym bezpečnostným incidentom, stratám dát a výpadkom kritických služieb, čo by malo negatívny dopad na obyvateľov mesta a mohlo by viesť k vysokým finančným a reputačným stratám.	1. Žiadne počiatočné náklady spojené s implementáciou nových systémov alebo procesov. 2. Vyhneme sa zložitosti spojenej s plánovaním a realizáciou projektu.	1. Vysoké riziko bezpečnostných incidentov v dôsledku neadresovania existujúcich a budúcich hrozieb. 2. Potenciálne fatálne následky v prípade bezpečnostného incidentu vrátane straty dát, financií a dôvery verejnosti. 3. Nedostatočná príprava na budúce technologické a bezpečnostné výzvy, čo môže viesť k

			dlhodobým stratám a zvýšeným nákladom na nápravu.

Tabuľka 5 Alternatívy v biznisovej vrstve

Z týchto analýz je zrejmé, že hoci kompletná implementácia projektu vyžaduje vyššie počiatočné investície a značné úsilie, dlhodobé výhody výrazne prevyšujú potenciálne nevýhody, najmä pokiaľ ide o komplexne riešenie všetkých identifikovaných potreby a zabezpečenie adekvátnej úrovne ochrany pre mesto a jeho obyvateľov

3.9 Multikriteriálna analýza

Na základe uvedených alternatív a kontextu môžeme vytvoriť tabuľku MCA pre výber najvhodnejšej alternatívy pre projekt zvyšovania úrovne kybernetickej a informačnej bezpečnosti mesta Ružomberok. Táto analýza sa zameriava na splnenie biznisových požiadaviek bez technologických predpojatostí.

Kritérium (KO = kľúčové kritérium)	ZDÔVODNENIE KRITÉRIA	Mesto	Obyvatelia	IT Oddelenie
Komplexnosť riešenia (KO)	Projekt by mal adresovať všetky identifikované bezpečnostné hrozby a nedostatky.	X	X	X
Udržateľnosť riešenia (KO)	Riešenie musí byť udržateľné a schopné adaptácie na budúce zmeny a hrozby.	X		X
Nákladová efektívnosť	Projekt by mal byť nákladovo efektívny pri zohľadnení dlhodobých výhod a rizík.	X		X
Zvýšenie kybernetickej odolnosti	Projekt by mal významne zvýšiť kybernetickú odolnosť mesta.	X	X	X
Minimálne narušenie existujúcich procesov	Projekt by mal minimalizovať narušenie existujúcich biznis procesov.			X

Tabuľka 6 Multikriteriálna analýza - Stanovenie kritérií

V tejto tabuľke:

- "Mesto" reprezentuje záujmy samosprávy, ktorá zodpovedá za celkovú kybernetickú a informačnú bezpečnosť a infraštruktúru.
- "Obyvatelia" predstavujú záujmy občanov mesta, ktorí sú priamymi užívateľmi mestských služieb, a pre ktorých je dôležitá ochrana ich osobných údajov a dostupnosť služieb.
- "IT Oddelenie" je zodpovedné za implementáciu a správu bezpečnostných riešení a IT infraštruktúry.

Zoznam kritérií	**Alternatíva 1: Realizácia projektu v plnej miere**	**Spôsob dosiahnutia**	**Alternatíva 2: Čiastočná implementácia projektu**	**Spôsob dosiahnutia**	**Alternatíva 3:** Udržiavanie súčasného stavu	**Spôsob dosiahnutia**
Komplexnosť	áno	Plná implementácia	nie		nie	

riešenia (KO)		zabezpečí komplexné riešenie všetkých identifikovaných problémov.				
Udržateľnosť riešenia (KO)	áno	Riešenie je navrhnuté tak, aby bolo udržateľné a adaptabilné na budúce zmeny.	nie		nie	
Nákladová efektívnosť	áno	Optimalizácia nákladov prostredníctvom efektívneho využívania zdrojov.	áno	Menej nákladové, ale aj menej efektívne.	nie	
Zvýšenie kybernetickej odolnosti	áno	Komplexné bezpečnostné opatrenia zvyšujú celkovú odolnosť.	nie		nie	
Minimálne narušenie existujúcich procesov	áno	Navrhnuté tak, aby minimalizovalo narušenie.	nie		nie	

Tabuľka 7 Multikriteriálna analýza - Porovnanie alternatív na základe naplnenia stanovených kritérií

Tabuľka poskytuje porovnanie, ako každá z alternatív spĺňa zvolené kritériá. Alternatíva 1 (úplná realizácia projektu) je jednoznačne preferovaná, keďže spĺňa všetky kritériá, zatiaľ čo alternatívy 2 a 3 majú významné nedostatky vo viacerých kľúčových oblastiach.

3.10 Stanovenie alternatív v aplikačnej vrstve architektúry

Alternatíva	Nutné moduly	Preferované moduly
Alternatíva 1: Realizácia projektu v plnej miere	• Plná implementácia SIEM systému so všetkými funkčnosťami pre detekciu, analýzu a reakciu na bezpečnostné incidenty. • Plná implementácia NGFW. • Rozsiahla modernizácia serverovej a sieťovej infraštruktúry.	• Rozšírené analytické a prediktívne schopnosti SIEM systému. . • Využitie cloudových technológií pre zvýšenie flexibility a škálovateľnosti IT infraštruktúry. •
Alternatíva 2: Čiastočná implementácia projektu	• Základná implementácia SIEM systému s obmedzenými analytickými schopnosťami. • Základná verzia NGFW, ktorá pokrýva iba čiastočnú funkcionalitu. • Obmedzená modernizácia serverovej a sieťovej infraštruktúry.	Preferované moduly alternatívy 2 sú v časti nutné moduly alternatívy 1.
Alternatíva 3: Udržiavanie súčasného stavu	Žiadne nové implementácie, udržiavanie existujúcich systémov a infraštruktúry bez zmien.	Neaplikuje sa, keďže žiadne nové moduly ani funkcionality nebudú pridané

Tabuľka 8 Alternatívy v aplikačnej vrstve

Tieto aplikačné alternatívy sa priamo odvíjajú od biznis alternatív a sú zamerané na konkrétne technologické riešenia, ktoré majú podporovať stanovené biznis ciele a požiadavky.

3.11 Stanovenie alternatív v technologickej vrstve architektúry

Technologická architektúra nemá definované varianty. Preferované sú riešenia prevádzkované "on premise" z dôvodu plnej kontroly nad technologickou infraštruktúrou a zabezpečenia vyššej miery prispôsobenia a integrácie s existujúcimi systémami, čo je zásadné pre splnenie špecifických bezpečnostných a regulačných požiadaviek. Zároveň prevádzka "on premise" riešení predstavuje nižšie dlhodobé prevádzkové náklady v porovnaní s neustálymi poplatkami za cloudové služby, čo je pre mesto z hľadiska udržateľnosti jeden z kľúčových faktorov.

4. POŽADOVANÉ VÝSTUPY (PRODUKT PROJEKTU)

Po ukončení projektu "" Podpora v oblasti kybernetickej a informačnej bezpečnosti v meste Ružomberok " budú dodané:

- Projektové výstupy podľa vyhlášky 401/2023 o riadení projektov, vrátane: Zdrojových kódov všetkých vyvinutých alebo modifikovaných aplikácií a systémov.
- Dokumentácie k implementovaným systémom a infraštruktúre, vrátane technickej, používateľskej a údržbovej dokumentácie.
- Protokoly z testovania a validácie systémov.
- V rámci hlavnej aktivity projektu sa budú realizovať nasledovné opatrenia s danými výstupmi:

Č.	Názov opatrenia	Popis	Výstup	Dopad/následok
1.	**Aktualizácia analýzy rizík**	Aktualizácia analýzy rizík zabezpečí správu aktív, zraniteľností, hrozieb a opatrení. Analýza rizík umožní aktualizovanie a hodnotenie rizík založené na aktuálnych dátach a poskytne nástroje pre efektívne riadenie a minimalizáciu rizík.	1. Aktualizácia analýzy rizík, hrozieb a zraniteľností, ktorej výsledky budú slúžiť ako východisko pre klasifikáciu informácií, kategorizáciu sietí a informačných systémov. 2. Aktualizácia klasifikácie informácií a kategorizácie sietí a informačných systémov, podľa klasifikačnej schémy v súlade s prílohou č.2 vyhlášky 362/2018.	*- zníženie zraniteľnosti vyplývajúcej s nedostatočného riadenie rizík a opatrení v oblasti KB*
2.	**Vybudovanie SIEM**	Monitorovanie hrozieb v reálnom čase prostredníctvom systémov ako SIEM, zabezpečí rýchlu reakciu na potenciálne bezpečnostné incidenty a výrazne prispieva k celkovej odolnosti mesta.	1. Implementácia SIEM 2. Dokumentácia a školenie.	*- zníženie zraniteľnosti - zrýchlenie reakcie pri bezpečnostných incidentoch (okamžité upozornenia na neobvyklé udalosti)*
3.	**Vypracovanie a implementácia komplexného plánu kontinuity činností**	Vypracovanie a implementácia plánu kontinuity činností (BCM), ktorý zahŕňa postupy pre rýchlu obnovu kritických systémov a služieb po narušení. Plán bude obsahovať scenáre pre rôzne typy udalostí a zahrnie analýzu funkčných dopadov, strategické zdroje na obnovu a časové rámce pre reakciu.	1. Plán kontinuity činností musí obsahovať minimálne: a. Plán kontinuity na stanovenie požiadaviek a zdrojov b. Plán reakcie na incidenty a plány havarijnej obnovy prevádzky c. Politiku a ciele kontinuity d. Analýzu funkčných dopadov e. Stratégiu riadenia kontinuity vrátane evakuačných postupov f. Plán údržby a kontroly BCMS. 2. Školenie	*- zníženie zraniteľnosti - zrýchlenie reakcie pri bezpečnostných incidentoch (okamžité upozornenia na neobvyklé udalosti)*
4.	**Modernizácia sieťovej infraštruktúry v mestskej informačnej sieti**	Zabezpečí sa výmena zastaraných sieťových prvkov, dobudovanie záložných trás a rozšírená segmentácia siete. Tieto kroky významne prispejú k zníženiu zraniteľností vyplývajúcich z používania EOL zariadení a ich nedostatočného zabezpečenia.	1. Vstupná analýza existujúcej sieťovej infraštruktúry a návrhu opatrení v zmysle vyhlášky NBU č.362/2018. 2. Výmena a inštalácia zastaralých sieťových prvkov na úrovni L2/L3. 3. Rekonfigurácia siete vrátane rozšírenej segmentácie a rozdelenia na VLAN. 4. Vytvorenie alebo aktualizácia dokumentácie počítačovej siete, ktorá obsahuje evidenciu všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológiu siete a využitie IP rozsahov 5. Zaškolenie IT personálu	*- zníženie zraniteľnosti vyplývajúcej z použitia EOL zariadení (nedostatočné zabezpečenie)* *- zníženie zraniteľnosti vyplývajúcej nízkej dostupnosti poskytovania základnej služby.*

5.	**Modernizácia serverovej infraštruktúry**	Výmena serverových komponentov, sieťových prvkov prispeje k zníženiu rizika nízkej dostupnosti poskytovania základnej služby a zraniteľnosti spojenej s používaním zastaraných zariadení.	1. Výmena serverov. 2. Výmena sieťových prvkov pre iSCSI. 3. Nasadenie platformy pre beh VM 4. Kompletná konfigurácia, dokumentácia a , zaškolenie IT pracovníkov 5. Montáž, inštalácia serverov a storage a ich prepojenie, nastavenie Domény, konfigurácia Active Directory, migrácia dát a migrácia databáz. 6. Aktualizácia, vypracovanie a dodanie príslušnej systémovej a používateľskej dokumentácie k vykonaným zmenám 7. Zaškolenie IT personálu	*- zníženie zraniteľnosti vyplývajúcej z použitia EOL zariadení (nedostatočné zabezpečenie)* *- zníženie zraniteľnosti vyplývajúcej nízkej dostupnosti poskytovania základnej služby.*
6.	**Zavedenie a správa nástroja na riadenie kapacít**	Nástroj na riadenie kapacít umožní nepretržité sledovanie všetkých IT aktív, poskytovanie včasných upozornení na potenciálne problémy a umožní rýchlu reakciu na incidenty. Týmto spôsobom sa zlepší viditeľnosť a kontrolu nad IT infraštruktúrou, čím sa zabezpečí jej spoľahlivú a bezpečnú prevádzku.	1. Inštalácia a základná konfigurácia. 2. Nastavenie monitorovacích objektov. 3. Konfigurácia upozornení a eskalácií. 4. Vizuálne rozhrania a reporty 5. Integrácia a rozšírenia. 6. Bezpečnosť a prístupové práva. 7. Školenie a podpora.	*- zníženie zraniteľnosti - zrýchlenie reakcie pri bezpečnostných incidentoch (okamžité upozornenia na neobvyklé udalosti)*
7.	**Nastavenie zálohovania**	Zavedenie stratégie a plánov zálohovania zabezpečí zvýšenie dostupnosti základnej služby.	1. Analýza a plánovanie zálohovania 2. Konfigurácia zálohovacieho softvéru 3. Automatizácia a monitorovanie. 4. Testovanie a validácia zálohovania 5. Školenie a dokumentácia	*- zníženie zraniteľnosti vyplývajúcej s potencionálnej straty údajov (zlyhanie HW, ransomware atd.)*
8.	**Dodanie a implementácia next-gen firewall technológie**	Umožní pokročilé filtrovanie obsahu, riadenie prestupov medzi sieťovými segmentami a integráciu s aktuálnymi bezpečnostnými systémami	Dodanie a implementácia next-gen firewall technológie vrátane: 1. Analýza súčasného stavu 2. Návrh implementačného konceptu a dizajnu riešenia 3. Inštalácia nového HW v priestoroch objednávateľa 4. Základná konfigurácia FW (IP adresa, názov, zóny, manažment ....) 5. Vytváranie nových pravidiel podľa pripraveného konceptu 6. Konfigurácia VPN tunelov 7. Migrácia objektov, smerovania, NAT 8. Migrácia komunikačných pravidiel 9. Integrácia so všetkými prvkami sieťovej infraštruktúry 10. Testovanie riešenia v testovacom prostredí 11. Migrácia do produkčného prostredia 12. Vyriešenie komunikačných problémov (prepojenie na externé subjekty, portály a pod. 13. Z inštalácie a kompletnej konfigurácie zariadenia 14. Aktualizácia, vypracovanie a	– *zníženie zraniteľnosti vyplývajúcej z nedostatočnej kontroly obsahu, monitorovania a analýzy informácií (únik informácií z vnútra, bezpečnostné incidenty)* – *zníženie zraniteľnosti vyplývajúcej z potencionálnych sieťových útokov na infraštruktúru MsÚ (DDoS, password attack, spoofing, neautorizovaný prístup..)*

			dodanie príslušnej systémovej a používateľskej dokumentácie k vykonaným zmenám 15. Zaškolenie IT personálu	
9.	**Vykonanie auditu kybernetickej bezpečnosti**	Vykonanie auditu a na začiatku a na konci projektu poskytne hodnotný prehľad o efektívnosti prijatých opatrení a pomôže identifikovať ďalšie možnosti zlepšenia.	1. Audit kybernetickej bezpečnosti v zmysle platného zákona o kybernetickej bezpečnosti. a. Vykonaný audit b. Záverečná správa o výsledkoch vykonaného auditu	- *vyhodnotenie dopadu prijatých opatrení na zvýšenie kybernetickej bezpečnosti*

V nasledujúcej tabuľke sú definované jednotlivé výstupy podľa vyhlášky 401/2023 o riadení projektov po fázach projektu pre každú etapu:

Etapy	**Požadované výstupy**
Analýza a dizajn	• Projektový iniciálny dokument (PID) • Akceptačné kritériá
	• Detailný návrh riešenia (DNR) o Zámer riešenia, analýza požiadaviek, používateľský prieskum a motivačná architektúra o Popis postupu analýzy a návrhu riešenia o Biznis architektúra o Dátová architektúra o Aplikačná architektúra o Technologická architektúra o Softvérové licencie a zdrojové kódy o Požiadavky na úrovne služieb (SLA) a výkonnosť o Zabezpečenie dostupnosti, zálohovanie a obnova riešenia o Bezpečnosť – riešenie požiadaviek na bezpečnosť o Migrácia dát o Harmonogram realizácie a nasadenia, závislosti
	• Plán a stratégia testovania o Testovacie prípady (UC/TC) o Testovacie prostredia o Testovacie dáta o Defekt manažment, monitoring a reporting testov
Implementácia a testovanie	• Vývoj, migrácia údajov a integrácia
	• Testovanie o Funkčné testovanie (FAT) o Systémové a integračné testovanie (SIT) o Záťažové a výkonnostné testovanie voliteľné o Bezpečnostné testovanie (SW/HW a kybernetická bezpečnosť) o Používateľské testy funkčného používateľského rozhrania (UX) o Používateľské akceptačné testovanie (UAT)
	• Školenia personálu
	• Dokumentácia o Aplikačná príručka o Integračná príručka o Používateľská príručka o Zdrojové kódy a licencie o Inštalačná a konfiguračná príručka

	○ Prevádzkový opis a pokyny pre diagnostiku, servis a údržbu ○ Pokyny na obnovu pri výpadku alebo havárii (Havarijný plán) ○ Bezpečnostný projekt voliteľné ○ Údaje o monitorovaní úrovne poskytovaných služieb (SLA) aktív IT
Nasadenie a postimplementačná podpora	• Nasadenie do produkčnej prevádzky (vyhodnotenie)
	• Akceptácia spustenia do produkčnej prevádzky (vyhodnotenie)
Dokončovacia fáza	• Manažérske správy, plány, reporty, zoznamy, odporúčania a požiadavky: ○ Správa o dokončení projektu (etapy/fázy) ○ Plán kontroly po odovzdaní projektu ○ Odporúčanie nadväzných krokov ○ Plán monitorovania a hodnotenia po odovzdaní projektu

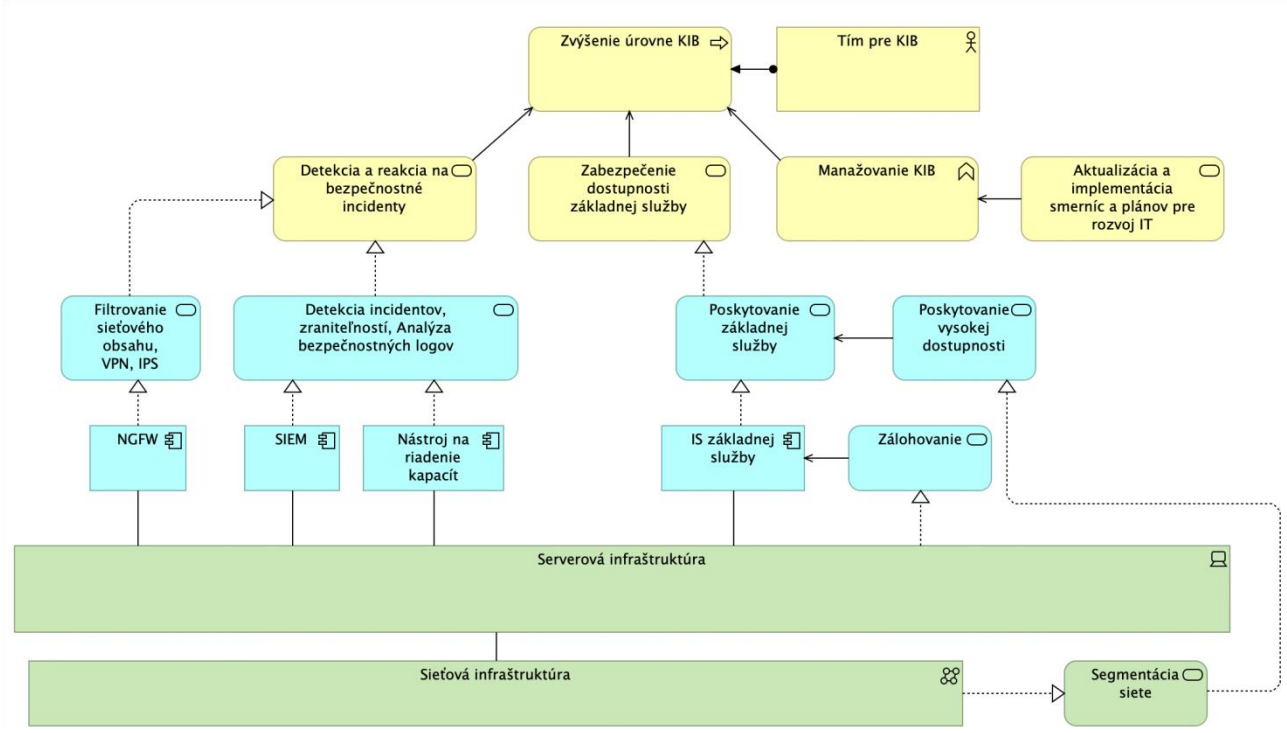
Tabuľka 9 Výstupy projektu podľa vyhlášky 401/2023 o riadení projektov po jednotlivých fázach pre každú etapu

Vlastníci procesov:

- IT oddelenie mesta: Zodpovedné za správu a údržbu IT infraštruktúry, vrátane zabezpečenia a monitorovania systémov.
- Manažér pre kybernetickú bezpečnosť: Zodpovedný za implementáciu a riadenie bezpečnostných systémov, ako napr. SIEM.

Títo vlastníci procesov budú mať kľúčovú úlohu pri riadení projektu a schvaľovaní jeho výstupov, zabezpečujúc, že realizované riešenia spĺňajú stanovené ciele a požiadavky mesta.

5. NÁHĽAD ARCHITEKTÚRY



Obrázok 2 Náhľad architektúry v notácii ArchiMate

Táto architektúra predstavuje komplexný prístup k zabezpečeniu kybernetickej a informačnej bezpečnosti v meste. Zahrnuté komponenty a služby sú navrhnuté tak, aby spolu synergicky pracovali na posilnení ochrany pred kybernetickými hrozbami a zabezpečení citlivých údajov.

V biznis vrstve máme "Zvýšenie úrovne KIB" ktorému slúžia služby Detekcia a reakcia na bezpečnostné incidenty, Zabezpečenie dostupnosti základnej služby a Manažovanie KIB ktoré sú nevyhnutné pre efektívne riadenie bezpečnostných rizík a zabezpečenie dôvernosti dát. Tieto procesy sú podporované tímom pre kybernetickú bezpečnosť, čo zabezpečuje, že organizácia má potrebné odborné znalosti a zdroje na riadenie a implementáciu bezpečnostných stratégií. Aktualizácie a implementácia smerníc a plánov pre rozvoj IT je dôležitou pre zabezpečenie správneho manažmentu KIB v meste.

V aplikačnej vrstve sú implementované kľúčové technologické riešenia:

- **SIEM** systém poskytuje komplexnú detekciu incidentov a analýzu bezpečnostných logov.
- **NGFW** zabezpečuje filtrovanie sieťového obsahu, VPN a IPS.

- **Nástroj na riadenie kapacít** zabezpečuje monitoring IT infraštruktúry

Tieto systémy sú základnými stavebnými blokmi pre detekciu a reakciu na potenciálne hrozby a incidenty.

Na technologickej vrstve je umiestnená serverová a sieťová infraštruktúra, ktoré poskytujú potrebné hardvérové a sieťové zdroje pre fungovanie aplikačných komponentov. Sieťová infraštruktúra poskytuje okrem komunikačnej funkcie prostredníctvom služby segmentácia vysokú dostupnosť pre poskytovanie základnej služby. Zálohovanie je zabezpečené prostredníctvom serverovej infraštruktúry.

Táto architektúra zabezpečuje, že mesto je schopné proaktívne čeliť kybernetickým hrozbám, ochraňovať svoje dáta a udržiavať nepretržitú operáciu svojich kritických služieb, čím prispieva k vyššej úrovni bezpečnosti a dôvery verejnosti v digitálne služby mesta.

6. LEGISLATÍVA

Pri návrhu a implementácii riešenia budeme vychádzať z nasledujúcej legislatívy:

PRÍRUČKY PROGRAMU SLOVENSKO
Príručka pre žiadateľa
Príručka pre prijímateľa (vrátane jej príloh)
Príručka k oprávnenosti výdavkov (vrátane jej príloh)
Komunikačná stratégia Program Slovensko programové obdobie 2021-2027 (vrátane jej príloh)
Všeobecná informácia k predkladaniu a schvaľovaniu ŽoNFP
Dizajn manuál Programu Slovenso (vrátane jej príloh)
Vzor Zmluvy o poskytnutí NFP
Príručka pre žiadateľov/prijímateľov k procesu a kontrole verejného obstarávania/obstarávania
ŠTANDARDY pre eGOVERNMENT
Zákon č. 95/2019 Z.z. o ITVS
Zákon č. 305/2013 Z.z. o eGovernmente a o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci
Zákon č. 177/2018 Z.z. proti byrokracii a o niektorých opatreniach na znižovanie administratívnej záťaže využívaním ISVS
Zákon č. 18/2018 Z.z. o ochrane osobných údajov
Vyhláška č. 85/2020 Z.z. o riadení IT projektov
Vyhláška č. 78/2020 Z.z. o štandardoch pre ITVS
Vyhláška č. 438/2019 Z.z. o výkone ustanovení zákona o e-Governmente (eDesk modul)
Vyhláška č. 331/2018 Z.z. o zaručenej konverzii
Vyhláška č. 29/2017 Z.z. o alternatívnom autentifikátore
Vyhláška č. 85/2018 Z.z. o spôsobe vyhotovenia listinného rovnopisu elektronického úradného dokumentu
Vyhláška č. 25/2014 Z.z. o IOM
Metodické usmernenie nariadeniu (GDPR) k spracúvaniu osobných údajov (prostredníctvom web stránok) v súlade s požiadavkami Nariadenia Rady EÚ č. 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov
Štandardné zmluvné doložky pre sprostredkovateľov (UOOU)
ŠTANDARDY pre KYBERNETICKÚ a INFORMAČNÚ BEZPEČNOSŤ
Zákon č. 69/2018 Z.z. o Kybernetickej bezpečnosti
Zákon č. 45/2011 Z.z. o Kritickej infraštruktúre
Zákon č. 351/2011 Z.z. o elektronických komunikáciách (ochrana súkromia a osobných údajov, ochrana sietí a zariadení)
Zákon č. 272/2016 Z.z. o dôveryhodných službách (elektronický podpis) a o dôveryhodných službách pre elektronické transakcie na vnútornom trhum (EiDAS)
Trestný zákon č. 300/2005 Z.z. (trestné činy páchané pomocou elektronických prostriedkov a v elektronickom prostredí)
Vyhláška č. 179/2020 Z.z. k spôsobom kategorizácie a obsahu bezpečnostných opatrení ITVS
Metodika pre Systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti (CSIRT)
Smernica č. 7/2019 o riešení Bezpečnostných incidentov Vládnou jednotkou CSIRT
Vyhláška NBU č. 166/2018 Z.z., o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov
Vyhláška NBU č. 164/2018 Z.z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby)
Vyhláška NBU č. 362/2018 Z.z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
Vyhláška NBU č. 436/2019 Z.z., o audite kybernetickej bezpečnosti a znalostnom štandarde audítora
ŠTANDARDY pre VLÁDNY CLOUD
Katalóg služieb a požiadavky na realizáciu služieb Vládneho Cloudu
Metodické usmernenie pre proces zaradenia cloudovej služby do katalógu č. 4542/2019/oSAEG-1

Usmernenie na aktualizáciu plánu migrácie IKT rezortu do dátového centra štátu
ŠTANDARDY pre RIADENIE PROJEKTU a PROGRAMU
Metodický pokyn k spracovaniu: _Štúdie uskutočniteľnost (ŠÚ) _Finančnej analýzy projektu _Analýzy nákladov a prínosov projektu (CBA) _Finančnej analýzy žiadateľa o NFP _Celkových nákladov na vlastníctvo v programovom období 2014 – 2020
Metodický pokyn UPVII č. 3425/2019/oPK-1 na rozpočtovanie nákupu IT v rámci medzirezortného programu 0EK Informačné technológie financované zo štátneho rozpočtu
Metodické usmernenie o postupe pri príprave investícií a koncesií podliehajúcich hodnoteniu MFSR
Rámec na hodnotenie verejných investičných projektov v SR
Používatelská priručka MetaIS
Používatelská príručka MetaIS Confluence
Informatizácia 2.0 - revízia výdavkov
ŠTANDARDY pre RIADENIE ARCHITEKTÚRY
Používateľská príručka MetaIS č. 3642/2018/oSAEG-1
Metodický pokyn ÚPVII č. 514/2017-313 z 10.1.2017 na aktualizáciu obsahu centrálneho metainformačného systému verejnej správy povinnými osobami v znení neskorších predpisov
Metodické usmernenie č. 5651/2019/oSAEG-1 z 20.09.2019 na odpočet plnenia NKIVS orgánmi riadenia
Pravidlá publikovania elektronických služieb do multikanálového prostredia verejnej správy (Číslo: 3204/2018/oAeG-1)
ŠTANDARDY pre KVALITU ÚDAJOV
Zákon č. 305/2013 Z.z. o eGovernmente (§52) - povinnosť referencovania sa a využívať referenčné údaje.
Zákon č. 305/2013 Z.z. o eGovernmente (§10) - povinnosť využívať „Modul procesnej integrácie a integrácie údajov (jeho časti IS CSRÚ)" a realizovať integráciu údajov, synchronizáciu údajov pri referencovaní a pri výmene údajov s referenčnými registrami a základnými číselníkmi.
Metodické umernenie o postupe zaraďovania referenčných údajov do zoznamu referenčných údajov vo väzbe na referenčné registre (č. 3639/2019/oDK-1)
Metodické usmernenie č. 1/2019 k zálohovaniu údajov v databázach domén, registrátorov a kontaktov súvisiacich so správou domén najvyššej úrovne
Postup pripojenia OVM v roli konzumenta údajov do IS CSRÚ
ŠTANDARDY pre DIZAJN a OPTIMALIZACIU PROCESOV a ŽIVOTNÝCH SITUÁCII
Metodika Používateľské princípy pre návrh a rozvoj elektronických služieb verejnej správy
Metodika optimalizácie procesov verejnej správy (najmä postupovať podľa bodu 3.5 b) pri vytváraní Procesnej analýzy) a v súlade s Metodikou optimalizácie procesov – konvenciami modelovania (aktualizovať diagramy životných situácií a karty životných situácií vedených na MVSR, ak Dielo ovplyvní výkon procesov životnej situácie)
Metodika merania výkonnosti procesov prostredníctvom KPI (dodať funkcionalitu exportu dát z Diela a meriania výkonnosti procesov)
Metodika merania nákladovosti TB-ABC
Metodika identifikácie, vizualizácie a referencovania údajov pri dátovom modelovaní vo verejnej správe
ŠTANDARDY pre UX
Metodika Jednotný dizajn manuál elektronických služieb verejnej správy
Metodické usmernenie UVSR č. 002089/2018/oLŠISVS-7 zo dňa 11.05.2018
Metodické usmernenie pre tvorbu používateľsky kvalitných elektronických služieb verejnej správy (Číslo spisu v DKS: 004307/2019/oBI)
ŠTANDARDY RIADENIA KVALITY
Metodika riadenia QAMPR
Riadenie kvality podľa Smernice STN EN ISO 9001: 2016
ŠTANDARDY pre LICENCIE
Uznesenia vlády č. 286/2019 o povinnosti prednostne pristupovať k platným a účinným centrálnym IKT zmluvám
Metodický pokyn k zabezpečeniu centrálneho nákupu produktov a služieb spoločnosti ORACLE v rámci Centrálnej rámcovej dohody na poskytovanie licencií a produktov ORACLE a služieb s nimi súvisiacich
ŠTANDARDY OBSTARAVANIA
Zákon č.343/2015 Z.z. o verejnom obstarávaní
Koncepcia nákupu IT vo verejnej správe (v kontexte rokovania o licencnych pravach k zdrojovemu kodu)
OSTATNÉ ŠTANDARDY
Zákon č. 211/2000 Z.z. o slobodnom prístupe k informáciám
Zákon č. 315/2016 Z.z. o registri partnerov verejného sektora

Tabuľka 10 Zoznam legislatívy

7. HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU A METÓDA JEHO RIADENIA

ID	FÁZA/AKTIVITA	ZAČIATOK (odhad termínu)	KONIEC (odhad termínu)
1.	Prípravná fáza a Iniciačná fáza	05/2024	12/2024
2.	Realizačná fáza	01/2025	12/2025
3.	Dokončovacia fáza	12/2025	12/2025
4.	Podpora prevádzky (SLA)	01/2026	12/2030

Tabuľka 10 Harmonogram projektu

Projekt sa realizuje metódou Waterfall s logickými nadväznosťami realizácie jednotlivých modulov na základe funkčnej a technickej špecifikácie vypracovanej v rámci prípravy projektu. Niektoré opatrenia sa budú realizovať paralelne, dokonca rôznymi tímami, avšak na základe vopred stanovej stratégie a plánu celého projektu.

Agilný prístup bol vylúčený s ohľadom na potrebu realizácie projektu za plnej prevádzky základnej služby Mesta Ružomberok.

Prípravná a Iniciačná fáza zahŕňa prípravu obsahu projektu, prípravu Manažérskych produktov v zmysle požiadaviek výzvy, definovanie zloženia projektového tímu a Riadiaceho výboru, príprava žiadosti o NFP. Iniciačná fáza bude ukončená schválením žiadosti o NFP a podpisom Zmluvy o poskytnutí NFP. Následne sa bude realizovať verejné obstarávanie, ktoré bude ukončené pred začiatkom hlavnej aktivity projektu.

V rámci realizačnej fázy sa bude realizovať obsah projektu /vyššie popísané/ s cieľom dosiahnutia hlavných cieľov a merateľných ukazovateľov. Taktiež sa bude pripravovať dokumentácia v zmysle požiadaviek definovaných vo Vyhláške 401/2023 Z.z. o riadení projektov.

Dokončovacia fáza vytvorí dokumenty a podklady pre ZMS, ako aj dokumenty v rámci požiadaviek Vyhlášky 401/2023 Z.z. stanovené pre dokončovaciu fázu.

Po uzatvorení dokončovacej fázy začne podpora prevádzky /totožná s obdobím udržateľnosti projektu/. Mesto Ružomberok zabezpečí využívanie implementovaných systémov a udržiavanie dosiahnutých výsledkov. Podpora bude zabezpečená aj uzatvorenými SLA zmluvami s dodávateľmi /pri podpore prevádzky/. Udržateľnosť projektu bude zabezpečená počas tohto obdobia vlastnými zdrojmi Mesta Ružomberok.

8. ROZPOČET A PRÍNOSY

Rozpočet bol zostavený na základe prieskumu trhu, ako výsledkov realizovania prieskumu s cieľom určenia predpokladanej hodnoty zákazky. V závislosti na výške rozpočtu projektu /do 1 000 000 Eur/ nebola spracovaná CBA analýza /Analýza nákladov a prínosov/.

Názov výdavku	MJ	Jednotková cena bez DPH (v EUR)	Počet jednotiek	Spolu s DPH (v EUR)
Analýza rizík	projekt	6 483,33 €	1	7 780,00 €
Zavedenie bezpečnostných a analytických systémov na monitorovanie hrozieb v reálnom čase. (SIEM)	projekt	47 000,00 €	1	56 400,00 €
Vypracovanie kontinuity činností v zmysle ZoKB	projekt	33 333,33 €	1	40 000,00 €
Návrh a segmentácia sieťovej infraštruktúry v informačnej sieti	projekt	94 966,67 €	1	113 960,00 €
Modernizácia serverovej infraštruktúry	projekt	158 666,67 €	1	190 400,00 €
Nástroj na riadenie kapacít	projekt	7 026,67 €	1	8 432,00 €
NGFW	ks	16 600,00 €	2	39 840,00 €
Nastavenie zálohovania	projekt	6 000,00 €	1	7 200,00 €
Vykonanie auditu kybernetickej bezpečnosti	projekt	8 133,33 €	1	9 760,00 €
Kľúčový používateľ	HOD	17,34 €	1975,5	33 943,05 €
Manažér kybernetickej bezpečnosti	HOD	23,84 €	1975,5	46 666,80 €

Paušálna sadzba	projekt	38 806,73 €	1	38 806,73 €
Celkový rozpočet				**593 188,58 €**

Vzhľadom na obsah projektu a definované ciele projektu /oblasť kybernetickej a informačnej bezpečnosti/ je pomerne náročné jednoznačne kvantifikovať návratnosť realizovanej investície. Realizované náklady primárne prispejú k zabezpečeniu poskytovania základnej služby, k minimalizovaniu zraniteľnosti systémov Mesta a zvýšeniu ochrany MsÚ. Z pohľadu návratnosti je však možné zdôrazniť hodnotenie možných škôd, ktoré by vznikli v prípade, že nebude vhodne riešená oblasť kybernetickej a informačnej bezpečnosti na úrovni PZS.

Jedná sa o nasledovné škody v závislosti na daných rizikách:

- **reputačné riziko** - v prípade neplnenia legislatívnych požiadaviek v zmysle Zákona o kybernetickej bezpečnosti a Zákona o ISVS a následného výpadku prevádzky základnej služby, či prípadného úniku citlivých a osobných údajov v kombinácii s prípadnou medializáciou je toto riziko pomerne vysoké v nadväznosti na zákonné povinnosti Mesta Ružomberok.
- **finančné riziko** /externé/- súvisí s možnými sankciami, pokutami vyplývajúce priamo z legislatívnych rámcov v rámci prípadných súdnych sporov /napr. pri úniku osobných údajov v súvislosti s kybernetickým útokom na MsÚ Ružomberok/. Výšku finančných sankcií/pokút nie je možné jednoznačne vyčísliť, keďže je závislá od rozsahu uniknutých informácií a ďalších faktorov. Môže však dôjsť k výraznému zaťaženiu rozpočtu Mesta Ružomberok.
- **finančné riziko** /interné/- súvisí s výpadkom poskytovania základnej služby, kedy zamestnanci úradu nebudú schopní pracovať so systémami mesta a zabezpečovať poskytovanie základnej služby. Celková strata v prípade výpadku poskytovania základne služby na úrovni straty miezd zamestnancov je závislá na dĺžke výpadku poskytovania základnej služby. Pri jednodňovom výpadku sa jedná približne o 9259,7 Eur pri 103 zamestnancoch /mesačná priemerná mzda verejnej správy v roku 2023 bola 1796 Eur, pri 20 dňovom pracovnom čase je priemerná denná mzda 89,9 Eur/.

9. PROJEKTOVÝ TÍM

Mesto Ružomberok v rámci prípravnej fázy zostavilo Riadiaci výbor v zmysle požiadaviek Vyhlášky 401/2023 Z.z., v nasledovnom zložení:

- Predseda Riadiaceho výboru - Ing. Richard Makovický/ referent grantov
- Zástupca prevádzky - Ing. Martin Žabenský/ vedúci IT oddelenia
- Biznis vlastník -. Mário Kľučka / prednosta Mestského úradu Ružomberok

Projektový tím v rámci projektu bol zostavený vzhľadom na obsah projektu a potrebu zabezpečenia podpory realizácie projektu interným prostredím Mesta Ružomberok. Na realizácii projektu budú participovať interní zamestnanci mesta, ktorí budú úzko kooperovať s externým dodávateľom v rámci implementácii konkrétnych opatrení popísaných v rámci realizácie projektu.

ID	Meno a Priezvisko	Pozícia	Oddelenie	Rola v projekte
4.	Ing. Richard Makovický	Referent grantov	Mesto Ružomberok	Kľúčový používateľ
5.	PhDr. Vladimíra Pazderová, PhD.	Projektový manažér	Externý poskytovateľ služby	Projektový manažér
6.	Ing. Martin Žabenský	Vedúci IT oddelenia	Kancelária prednostky MsÚ/Mesto Ružomberok	Manažér kybernetickej a informačnej bezpečnosti

Tabuľka 11 Projektový tím

9.1 PRACOVNÉ NÁPLNE

Projektová rola:	**MANAŽER KYBERNETICKEJ BEZPEČNOSTI**
Stručný popis:	• zodpovedá za dodržanie princípov a štandardov na kybernertickú a IT bezpečnosť, za kontrolu a audit správnosti riešenia v oblasti bezpečnosti. • koordinuje a riadi činnosť v oblasti bezpečnosti prevádzky IT, spolupracuje na projektoch, na rozvoji nástrojov a postupov k optimalizácii bezpečnostných systémov a opatrení. Stanovuje základné požiadavky, podmienky a štandardy pre oblasť bezpečnosti programov, systémov, databázy či sieti. Spracováva a kontroluje príslušné interné predpisy a dohliada nad plnením týchto štandardov a predpisov. Kontroluje a riadi činnosť nad bezpečnostnými testami, bezpečnostnými incidentmi v prevádzke IT. Poskytuje inštrukcie a poradenstvo používateľom počítačov a informačných systémov pre oblasť bezpečnosti

	PODMIENKY SPRÁVNEHO a EFEKTÍVNEHO VÝKONU ČINNOSTI role Manažér KYBERNETICKEJ BEZPEČNOSTI: 1) neobmedzený aktívny prístup ku všetkým projektovým dokumentom, nástrojom a výstupom projektu, v ktorých sa opisuje predmet projektu z hľadiska jeho architektúry, funkcií, procesov, manažmentu informačnej bezpečnosti a spôsobov spracúvania dát, ako aj dát samotných. 2) rola manažér Kybernetickej a IT bezpečnosti si vyžaduje mať sprístupnené všetky informácie o bezpečnostných opatreniach zavádzaných projektom v zmysle: a) § 20 zákona č.69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov b) ustanovení zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
Detailný popis rozsahu zodpovednosti, povinností a kompetencií	Zodpovedný za: • špecifikovanie štandardov, princípov a stratégií v oblasti KIB, • ak je projekt primárne zameraný na problematiku KIB – je priamo zodpovedný za špecifikáciu a analýzu funkčných požiadaviek na KIB, • špecifikovanie požiadaviek na KIB, kontroluje ich implementáciu v realizovanom projekte, • špecifikovanie požiadaviek na bezpečnosť vývojového, testovacieho a produkčného prostredia, • špecifikovanie funkčných a nefunkčných požiadaviek pre oblasť KIB, • špecifikovanie požiadaviek na bezpečnosť v rámci bezpečnostnej vrstvy, • špecifikovanie požiadaviek na školenia pre oblasť KIB, • špecifikovanie požiadaviek na bezpečnostnú architektúru riešenia a technickú infraštruktúru pre oblasť KIB, • špecifikovanie požiadaviek na dostupnosť, zálohovanie, archiváciu a obnovu IS vzťahujúce sa na KIB, • realizáciu posúdenie požiadaviek agendy KIB na integrácie a procesov konverzie a migrácie, identifikácia nesúladu a návrh riešenia • špecifikovanie požiadaviek na KIB, bezpečnostný projekt a riadenie prístupu, • špecifikovanie požiadaviek na testovanie z hľadiska KIB, realizáciu kontroly zapracovania a retestu, • špecifikovanie požiadaviek na obsah dokumentácie v zmysle legislatívnych požiadaviek pre oblasť KIB, ako aj v zmysle "best practies", • špecifikovanie požiadaviek na dodanie potrebnej dokumentácie súvisiacej s KIB kontroluje ich implementáciu v realizovanom projekte, • špecifikovanie požiadaviek a konzultácie pri návrhu riešenia za agendu KIB v rámci procesu „Mapovanie a analýza technických požiadaviek - detailný návrh riešenia (DNR)", • špecifikáciu požiadaviek na bezpečnosť KIB v rámci procesu "akceptácie, odovzdania a správy zdroj. kódov" • špecifikáciu akceptačných kritérií za oblasť KIB, • špecifikáciu pravidiel pre publicitu a informovanosť s ohľadom na KIB, • poskytovanie konzultácií pri tvorbe šablón a vzorov dokumentácie pre oblasť KIB, • získavanie informácií nutných pre plnenie úloh v oblasti KIB, • špecifikáciu podmienok na testovanie, reviduje výsledky a výstupy z testovania za oblasť KIB, • konzultácie a vykonávanie kontrolnej činnosť zameranej na obsah a komplexnosť dok. z hľadiska KIB, • špecifikáciu požiadaviek na bezpečnostný projekt pre oblasť KIB, • realizáciu kontroly zameranej na naplnenie požiadaviek definovaných v bezp. projekte za oblasť KIB • realizáciu kontroly zameranú na správnosť nastavení a konfigurácii bezpečnosti jednotlivých prostredí, • realizáciu kontroly zameranú realizáciu procesu posudzovania a komplexnosti bezpečnostných rizík, bezpečnosť a kompletný popis rozhraní, správnu identifikácia závislostí, • realizáciu kontroly naplnenia definovaných požiadaviek pre oblasť KIB, • realizáciu kontroly zameranú na implementovaný proces v priamom súvise s KIB, • realizáciu kontroly súladu s planou legislatívou v oblasti KIB (obsahuje aj kontrolu leg. požiadaviek) • realizáciu kontroly zameranú zabezpečenie procesu, interfejsov, integrácii, kompletného popisu rozhraní a spoločných komponentov a posúdenia z pohľadu bezpečnosti, • poskytovanie konzultácií a súčinnosti pre problematiku KIB, • získavanie a spracovanie informácií nutných pre plnenie úloh v oblasti KIB, • aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 85/2020 Z.z., Prílohou č.1 • plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

Projektová rola:	**PROJEKTOVÝ MANAŽÉR**
Stručný popis:	• zodpovedá za riadenie projektu počas celého životného cyklu projektu. Riadi projektové (ľudské a finančné) zdroje, zabezpečuje tvorbu obsahu, neustále odôvodňovanie projektu (aktualizuje BC/CBA) a predkladá vstupy na rokovanie Riadiaceho výboru. Zodpovedá za riadenie všetkých (ľudských a finančných) zdrojov, členov projektovému tím objednávateľa a za efektívnu komunikáciu s dodávateľom alebo stanovených zástupcom dodávateľa. • zodpovedá za riadenie prideleného projektu - stanovenie cieľov, spracovanie harmonogramu prác,

	koordináciu členov projektového tímu, sledovanie dodržiavania harmonogramu prác a rozpočtu, hodnotenie a prezentáciu výsledkov a za riadenie s tým súvisiacich rizík. Projektový manažér vedie špecifikáciu a implementáciu projektov v súlade s firemnými štandardami, zásadami a princípmi projektového riadenia. • zodpovedá za plnenie projektových/programových cieľov v rámci stanovených kvalitatívnych, časových a rozpočtovým plánov a za riadenie s tým súvisiacich rizík. V prípade externých kontraktov sa vedúci projektu/ projektový manažér obvykle podieľa na ich plánovaní a vyjednávaní a je hlavnou kontaktnou osobou pre zákazníka.
Detailný popis rozsahu zodpovednosti, povinností a kompetencií	Zodpovedný za: • Riadenie projektu podľa pravidiel stanovených vo Vyhláške 85/2020 Z.z. • Riadenie prípravy, inicializácie a realizácie projektu • Identifikovanie kritických miest projektu a navrhovanie ciest k ich eliminácii • Plánovanie, organizovanie, motivovanie projektového tímu a monitorovanie projektu • Zabezpečenie efektívneho riadenia všetkých projektových zdrojov s cieľom vytvorenia a dodania obsahu a zabezpečenie naplnenie cieľov projektu • Určenie pravidiel, spôsobov, metód a nástrojov riadenia projektu a získanie podpory Riadiaceho výboru (RV) pre riadenie, plánovanie a kontrolu projektu a využívanie projektových zdrojov • Zabezpečenie vypracovania manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 85/2020 Z.z., Prílohou č.1 • Zabezpečenie realizácie projektu podľa štandardov definovaných vo Vyhláške 78/2020 Z.z. • Zabezpečenie priebežnej aktualizácie a verzionovania manažérskej a špecializovanej dokumentácie v minimálnom rozsahu Vyhlášky 85/2020 Z.z., Prílohy č.1 • Vypracovanie, pravidelné predkladanie a zabezpečovanie prezentácie stavov projektu, reportov, návrhov riešení problémov a odsúhlasovania manažérskej a špecializovanej dokumentácie v rozsahu určenom Vyhláškou 85/2020 Z.z., Prílohou č.1 na rokovanie RV • Riadenie a operatívne riešenie a odstraňovanie strategických / projektových rizík a závislostí • Predkladanie návrhov na zlepšenia na rokovanie Riadiaceho výboru (RV) • Zabezpečenie vytvorenia a pravidelnej aktualizácie BC/CBA a priebežné zdôvodňovanie projektu a predkladanie na rokovania RV • Celkovú alokáciu a efektívne využívanie ľudských a finančných zdrojov v projekte • Celkový postup prác v projekte a realizuje nápravné kroky v prípade potreby • Vypracovanie požiadaviek na zmenu (CR), návrh ich prioritizácie a predkladanie zmenových požiadaviek na rokovanie RV • Riadenie zmeny (CR) a prípadné požadované riadenie konfigurácií a ich zmien • Riadenie implementačných a prevádzkových aktivít v rámci projektov. • Aktívne komunikuje s dodávateľom, zástupcom dodávateľa a projektovým manažérom dodávateľa s cieľom zabezpečiť úspešné dodanie a nasadenie požadovaných projektových výstupov, • Formálnu administráciu projektu, riadenie centrálneho projektového úložiska, správu a archiváciu projektovej dokumentácie • Kontrolu dodržiavania a plnenia míľnikov v zmysle zmluvy s dodávateľom, • Dodržiavanie metodík projektového riadenia, • Predkladanie požiadaviek dodávateľa na rokovanie Riadiaceho výboru (RV), • Vecnú a procesnú administráciu zúčtovania dodávateľských faktúr

Projektová rola:	**KĽUČOVÝ POUŽIVATEĽ** (end user)
Stručný popis:	• zodpovedný za reprezentáciu záujmov budúcich používateľov projektových produktov alebo projektových výstupov a za overenie kvality produktu. • zodpovedný 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. • Kľúčový používateľ (end user) navrhuje a definuje akceptačné kritériá, je zodpovedný za akceptačné testovanie a návrh na akceptáciu projektových produktov alebo projektových výstupov a návrh na spustenie do produkčnej prevádzky. Predkladá požiadavky na zmenu funkcionalít produktov a je súčasťou projektových tímov
Detailný popis rozsahu zodpovednosti, povinností a kompetencií	Zodpovedný za: • Návrh a špecifikáciu funkčných a technických požiadaviek • Jednoznačnú špecifikáciu požiadaviek na jednotlivé projektové výstupy (špecializované produkty a výstupy) z pohľadu vecno-procesného a legislatívy • Vytvorenie špecifikácie, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu, • Špecifikáciu požiadaviek koncových používateľov na prínos systému • Špecifikáciu požiadaviek na bezpečnosť, • Návrh a definovanie akceptačných kritérií, • Vykonanie používateľského testovania funkčného používateľského rozhrania (UX testovania) • Finálne odsúhlasenie používateľského rozhrania

	• Vykonanie akceptačného testovania (UAT) • Finálne odsúhlasenie a akceptáciu manažérskych a špecializovaných produktov alebo projektových výstupov • Finálny návrh na spustenie do produkčnej prevádzky, • Predkladanie požiadaviek na zmenu funkcionalít produktov • Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 85/2020 Z.z., Prílohou č.1 • Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

8. PRÍLOHY

Príloha 1 : Register rizík a závislostí - *PRILOHA_1_REGISTER_RIZIK-a-ZAVISLOSTI_Podpora_v_oblasti_KB_a_IB_Ruzomberok.xlsx*