PRÍSTUP K PROJEKTU

Vzor pre manažérsky výstup I-03

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

Povinná osoba	Mesto Banská Bystrica
Názov projektu	Zvýšenie úrovne kybernetickej a informačnej bezpečnosti Mesta Banská Bystrica
Zodpovedná osoba za projekt	Ing. Beáta Galková
Realizátor projektu	Mesto Banská Bystrica
Vlastník projektu	Ing. Bibiána Palušková

Schvaľovanie dokumentu

Položka	**Meno a priezvisko**	**Organizácia**	**Pracovná pozícia**	**Dátum**	**Podpis** (alebo elektronický súhlas)
Vypracoval	Ing. Beáta Galková Ing. Bibiána Palušková	Mesto Banská Bystrica	Referent	22.04.2024	

1. HISTÓRIA DOKUMENTU

Verzia	**Dátum**	**Zmeny**	**Meno**
0.1	03.04.2024	Draft pracovnej verzie	Ing. Beáta Galková
0.2	22.04.2024	Zapracované pripomienky z v 0.1	Ing. Beáta Galková

2. ÚČEL DOKUMENTU

Tento dokument slúži pre účely prípravnej fázy projektu **„Realizácia opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti v Meste Banská Bystrica“**. Dokument sumarizuje, analyzuje a ďalej rozpracúva informácie z pohľadu aktuálneho stavu do takej úrovne detailu, aby bolo možné rozhodnúť o pokračovaní prípravy projektu, alokovaní rozpočtových zdrojov, personálnych kapacít a kvalifikovane rozhodnúť o prechode do iniciačnej fázy projektu.

Dokument súčasne rámcovo popisuje spôsob riešenia formou jednotlivých vrstiev architektúry, ktoré sú s ohľadom na charakter projektového zámeru relevantnými. Dokument sa podrobne nevenuje popisu business procesov, popisu dátovej a aplikačnej architektúry, nakoľko realizáciou projektu sa **neočakáva vykonať zásah do týchto domén architektúr modelu „ADM“ podnikovej architektúry definovanej rámcom TOGAF®.**

Dokument súčasne zachytáva aspekty bezpečnostnej architektúry v kontexte sieťovej architektúry, na ktorú budú mať navrhované oblasti a aktivity projektu najzásadnejší dopad.

2.1 Použité skratky a pojmy

SKRATKA/POJEM	**POPIS**
IB	Informačná bezpečnosť
KB	Kybernetická bezpečnosť
2FA	Dvojfaktorové overovanie
HW	Hardvér
IKT	Informačno-komunikačné technológie
ISVS	Informačný systém verejnej správy
Mesto	Mesto Banská Bystrica
RV	Riadiaci výbor
SLA	Service Level Agreement
SW	Softvér

VO	Verejné obstarávanie
Zákon o KB	Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

2.2 Konvencie pre typy požiadaviek

Užívateľské požiadavky majú nasledovnú konvenciu:

U_nn_Rxx

- U – užívateľská požiadavka
- Nn – typ používateľa
- R – označenie požiadavky
- Xx – číslo požiadavky

Procesné požiadavky majú nasledovnú konvenciu:

P_ABXY_Rxx

- P - procesná požiadavka
- AB – označenie procesu
- XY – číslo podprocesu
- R – označenie požiadavky
- Xx – číslo požiadavky

Požiadavky na reporting majú nasledovnú konvenciu:

R_ABXY_Rxx

- R – požiadavka na reporting
- Nn – číslo reportu
- R – označenie požiadavky
- Xx – číslo požiadavky

3. POPIS NAVRHOVANÉHO RIEŠENIA

Predkladané riešenie bolo navrhnuté na základe vykonanej analýzy možných alternatívnych riešení pri súčasnom zohľadnení aktuálneho stavu v oblasti IB a KB v Meste Banská Bystrica. Pre stanovenie navrhovaného riešenia boli vykonané nasledovné vzájomne súvisiace úkony.

- Identifikácia a analýza nevyhnutných riešených oblastí zvýšenia úrovne informačnej bezpečnosti a kybernetickej bezpečnosti na podklade vykonaného auditu KB a opakovaného auditu KB;
- Sumarizácia možných oblastí podporujúcich zvýšenie úrovne IB a KB v organizácii, určenie úrovne priority ich realizácie s ohľadom na potrebu, možné dopady v oblasti IB a KB ako aj odhadované finančné, technické, personálne nároky;
- Selekcia konečného optimálneho setu oblastí v rámci, ktorých je potrebné vykonať nevyhnutné aktivity pre zvýšenie úrovne IB a KB v Meste Banská Bystrica;
- Realizácia alternatív na úrovni business vrstvy s cieľom stanovenia preferovaného variantu realizácie projektu a teda definovanie konečného rozsahu projektového zámeru a navrhovaného riešenia (viac viď kapitola 3.8 dokumentu „Projektový zámer“).

Projekt v kontexte horeuvedeného postupu navrhuje s cieľom zaistenia kybernetickej ochrany v podmienkach Mesta Banská Bystrica v súlade s ustanoveniami Zákona o KB riešiť oblasti IB a KB, ktoré priamo reflektujú na známe zistenia z už vykonaných auditov KB realizovaných v prostredí organizácie, tak aby projekt v čo najväčšej možnej miere prispel k zosúladeniu oblasti riadenia kybernetickej a informačnej bezpečnosti s požiadavkami a očakávaniami príslušných štátnych orgánov ako aj príslušných aktuálne platných legislatívnych požiadaviek. **Projekt realizácie opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti v Meste Banská Bystrica je zameraný na dobudovanie infraštruktúry, posilnenie kybernetickej bezpečnosti organizácie, zlepšenie procesov, komunikácie ako aj celkové uchytenie a zlepšenie úrovne governance v oblasti IB a KB v organizácii, zber a analýzu prevádzkových dát v sieti pre zamedzenie a/alebo efektívne riešenie prípadných bezpečnostných incidentov, zrýchlenie detekcie ako aj riešenia kybernetických incidentov pri ambícií posilnenia preventívnych opatrení nad následným incident/problem managementom.**

Iniciatíva projektu vychádza z viacerých základných predpokladov, ktoré sú vzájomne previazané:

- Nárast rizika kybernetických útokov zameraných na subjekty verejnej správy a prevádzkovateľov základnej služby;
- Potreba zvýšenia efektivity procesov riadenia informačnej a kybernetickej bezpečnosti rámci IKT organizácie;
- Potreba riešenia nedostatku kvalifikovaných odborných IKT špecialistov a špecialistov informačnej bezpečnosti a kybernetickej bezpečnosti prostredníctvom centrálnej správy, automatizácie a manažmentu procesov a aktív;
- Potreba zvýšenia transparentnosti a efektívnosti manažmentu výkonu prevádzky IKT v organizácii;
- Potreba zvýšenia visibility v monitorovaných IS prostredníctvom implementácie manažmentových a dohľadových nástrojov;
- Naplnenie zákonných a regulatívnych požiadaviek;
- Zvýšiť bezpečnosť siete prostredníctvom rozšírenia prístupových pravidiel pri zachovaní užívateľského komfortu;
- Absencia vykonania inventarizácie informačných aktív, vykonania klasifikácie a kategorizácie IS a sietí, vykonania AR a BIA ako aj absencia zabezpečenia formalizovaného a opakovaného procesu riadenia identifikovaných rizík (ich mitigácie), ktoré sú nevyhnutným a nutným predpokladom pre efektívne riadenie rizík IB a KB;
- Absencia bezpečnostných opatrení pre jednotlivé klasifikačné stupne a kategórie IS a absencia základnej sady dokumentácie požadovanej Zákonom o KB;
- Absencia základných smerníc pre výkon procesov riadenia IB a KB v rámci jednotlivých oblastí riadenia;
- Absencia ľudských kapacít na efektívny bezpečnostný monitoring, konsolidáciu logov a auditných záznamov, analýzu bezpečnostných udalostí a incidentov a aj na ich riešenie so súčasnou snahou odbúrania pracovnej záťaže prechodom na automatizáciu a digitalizáciu týchto procesov.

Hlavný cieľom projektu je **zaistenie kybernetickej ochrany v podmienkach Mesta Banská Bystrica v súlade s ustanoveniami Zákona o KB.** Pre naplnenie cieľov boli identifikované nasledovné aktivity, ktoré bude potrebné vykonať:

1. Vykonať opakovaný audit informačnej a kybernetickej bezpečnosti v súlade s § 29 Zákona o KB;
2. Vypracovať relevantnú bezpečnostnú dokumentáciu;
3. Implementovať a konfigurovať systém pre riadenie správy prístupov koncových zariadení do siete Mesta Banská Bystrica;
4. Vykonať segmentáciu siete Mesta Banská Bystrica s ohľadom na súčasné prevádzkové požiadavky;
5. Zrealizovať výmenu aktívnych prvkov CORE časti siete;
6. Implementovať systém dvojfaktorovej autentifikácie pre vzdialený prístup do vnútornej siete;
7. Implementovať riešenie centrálneho bezpečnostného manažmentu pre koncové stanice.

Paralelne s týmito aktivitami bude nevyhnutne potrebné v relevantných oblastiach vykonať školenia dotknutých stakeholderov na výstupy jednotlivých aktivít tak, aby bola zachovaná vysoká úroveň profesionality ako aj kontinuity prevádzky celého predmetu projektu.

Implementácia horeuvedených aktivít prispeje k celkovému zvýšeniu úrovne IB a KB v Meste Banská Bystrica a ako aj odstráneniu identifikovaných nesúladov, ktoré boli identifikované počas vykonaných auditov IB a KB. Súčasne sa od projektu očakáva prínos v oblasti zrýchlenia, identifikácie, analýzy hrozieb ako aj odstraňovania prípadných kybernetických incidentov. Projekt ako taký plne korešponduje so strategickým smerovaním Mesta Banská Bystrica v oblasti IB, KB a rozvoja IKT ako aj so strategickými dokumentami na národnej ako aj nadnárodnej úrovni, súlad s ktorými bol rovnako jedným z motivátorom realizácie projektu (viď kap 3 dokumentu Projektový zámer).

Popis navrhovaného riešenia/aktivít projektu

a. Vykonanie opakovaného auditu informačnej a kybernetickej bezpečnosti v súlade s § 29 Zákona o KB

Mesto Banská Bystrica v čase po vyhlásení výzvy: „Podpora v oblasti kybernetickej a informačnej bezpečnosti na regionálnej úrovni – verejná správa“, kód: PSK-MIRRI-611-2024-DV-EFRR zahájilo plánovaný opakovaný audit kybernetickej bezpečnosti v súlade s § 29 Zákona o KB. Audit KB prebieha v čase 04/2024 pričom už z jeho priebehu je známe potvrdenie zistených nesúladov v audite vykonávanom v predchádzajúcom období. Ambíciou Mesta Banská Bystrica je využiť jestvujúce auditné správy ako aj predbežné informácie a konzultácie z prebiehajúceho auditu na adresnejšie a účelnejšie definovanie priorít a potrieb v oblasti zabezpečenia vysokej úrovne zabezpečenia IB a KB na úrovni celej organizácie. Identifikované riziká a slabé miesta boli pri selekcii a prioritizácii navrhovaných aktivít kľúčovým vstupom pre celé uchopenie projektového zámeru s ohľadom na možné dopady v oblasti IB a KB ako aj s ohľadom na efektívnu alokáciu limitovaných finančných, technických a personálnych kapacít v kontexte najväčšej možnej dosiahnutej protihodnoty ako aj súladu s legislatívou v oblasti IB a KB. Bez pravidelnej aktualizácie stavu zabezpečenia IB a KB v organizácii by Mesto Banská Bystrica na jednej strane nespĺňala požiadavky zo Zákona o KB, ktoré sa kladú na prevádzkovateľa základnej služby a súčasne by nebolo možné poznať efektívne možnosti a spôsoby dosiahnutia vyššej úrovne zabezpečenia IB a KB ako aj úrovne governance v oblasti IB a KB. V neposlednom rade je vykonanie opakovaného auditu KB nevyhnutným predpokladom pre zlepšenie povedomia a vzdelávania o aspektoch IB a KB na úrovni celej organizácie a na úrovni dotknutých stakeholderov. Táto aktivita je s ohľadom na uvedené vyššie vnímaná ako nevyhnutná prerekvizita pre ostatné časti súvisiaceho navrhovaného riešenia.

2. Vypracovanie relevantnej bezpečnostnej dokumentácie

Mesto Banská Bystrica v súčasnosti nedisponuje žiadnou z povinnej dokumentácie v zmysle Vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných opatrení v znení vyhlášky č. 264/2023 Z.z. Z uvedeného dôvodu verejný obstarávateľ plánuje zabezpečiť vypracovanie relevantnej dokumentácie a zosúladenie so zákonnými požiadavkami kladenými na poskytovateľa základnej služby. V súčasnosti Mesto Banská Bystrica disponuje iba zriadeným bezpečnostným výborom, ale samotné riadenie informačnej bezpečnosti a kybernetickej bezpečnosti nie je vôbec formalizované. Predmetom zamýšľanej aktivity je vykonanie analýzy rizík („AR“) pre aktíva podporujúce základnú službu podľa štandardov medzinárodnej normy ISO/IEC 27005:2018 a metodiky uvedenej vo Vyhláške NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení („Vyhláška o KB“). Súčasne sa plánuje v rámci uvedenej aktivity vykonať analýzu dopadov kľúčových činností a vyhodnotenie ich parametrov ako aj pripraviť základné politiky riadenia kybernetickej bezpečnosti podľa Zákona o KB a Vyhlášky o KB. Zároveň je v pláne vypracovať dokumentáciu relevantnú pre oblasť riadenia kontinuity činností a procesov, súčasne s vypracovaním a otestovaním týchto plánov v podmienkach organizácie.

V rámci aktivity sa plánuje dodanie nasledovnej bezpečnostnej dokumentácie, ktorá bude vychádzať z aktuálneho stavu informačnej a kybernetickej bezpečnosti ako aj aktuálne platného legislatívneho rámca:

- Vykonanie inventarizácie aktív vrátane klasifikácie informácií a kategorizácie sietí a informačných systémov;
- Vypracovanie analýzy rizík („AR“) podľa požiadaviek uvedených vo Vyhláške o KB v súlade s metodikou medzinárodnej normy ISO/IEC 27005:2018. Aktivita bude súčasne zohľadňovať:
    - *relevantné hrozby;*
    - *aktíva podieľajúce sa na dodávke základnej služby;*
    - *relevantné a známe zraniteľnosti;*
    - *určenie pravdepodobnosti a odhad dopadov pri realizáciách hrozieb;*
    - *Stanovenie úrovne rizika;*
    - *Stanovenie miery účinkov bezpečnostných opatrení a úroveň reziduálneho rizika;*
    - *návrh opatrení na zníženie reziduálnych rizík, ktoré sú vyššie ako akceptovateľná miera definovaná vedením organizácie verejného obstarávateľa.*
    - *Vypracovanie sumárneho prehľadu kybernetických rizík v prostredí Mesta Banská Bystrica spolu s návrhom opatrení na ich zníženie s cieľom dosiahnutia akceptovateľnej miery rizika.*
- Vypracovanie analýzy dopadov a kľúčových procesov a činností („BIA“) zahrňujúcej analýzu biznis dopadov („BIA“), vrátane prípravy smernice/metodiky pre riadenie oblasti BCM, prípravy plánov BCM a plánov obnovy DRP vrátane testovania navrhnutých plánov s vybranými zamestnancami Mesta Banská Bystrica. Aktivita bude súčasne zohľadňovať:
    - *Určenie funkčných závislostí kľúčových procesov v prostredí Mesta Banská Bystrica a potrebných zdrojov pre udržanie kontinuity ich výkonu;*
    - *Určenie relevantných scenárov havárií;*
    - *určenie parametrov „cieľový čas obnovenia – Recovery Time Objective (RTO)“ a „cieľový bod obnovenia – Recovery Point Objective (RPO)“ pre jednotlivé kľúčové procesy;*
    - *Identifikácia kľúčových procesov, ich závislostí a parametrov potrebných pre návrh náhradných scenárov obnovy pri havárii.*
- Vypracovanie základných bezpečnostných politík KB podľa Prílohy č. 1 k Vyhláške o KB:
    - *Bezpečnostná stratégia kybernetickej bezpečnosti;*
    - *Politika organizácie bezpečnosti;*
    - *Politika pre riadenie bezpečnosti rizík;*
    - *Politika pre riadenie informačných aktív;*
    - *Pravidlá správania sa a dobrej praxe;*
    - *Politika pre riadenie dodávateľských vzťahov;*
    - *Politika pre riadenie vývoja a údržby v oblasti IKT;*
    - *Politika pre riadenie a prevádzku IKT;*
    - *Politika pre riadenie súladu;*
    - *Politika pre riadenie kontinuity procesov a činností.*

3. Implementácia a konfigurácia systému pre riadenie správy prístupov koncových zariadení do siete Mesta

Súčasťou tejto aktivity projektu bude nasadenie SW riešenia na centralizovanú autentifikáciu a autorizáciu pre rôzne typy používateľov a zariadení v sieti, správu politík prístupu na základe možnosti definície identít, rolí, zariadení, prípadne ďalších, správcom siete voliteľných atribútov. Riešenie umožní sledovať a revidovať prístupy používateľov do siete Mesta, správu prístupov do siete zariadeniami pristupujúcimi v režime BYOD („Bring Your Own Device“) – zariadení, ktoré nie sú v správe a priamej kontrole IKT Mesta. Implementované riešenie zjednotí, zjednoduší a urýchli správu prístupov v rámci siete Mesta Banská Bystrica a to prostredníctvom implementácie štandardu IEEE 802.1X pre autentifikáciu a autorizáciu zariadení, ktoré budú nadväzovať spojenie so sieťou Mesta. Správa prístupových práv a politík sa plánuje realizovať na úrovni portov aktívnych sieťových prvkov. Súčasťou tejto bude dodávka aktívnych sieťových prvkov vrátane realizácie inštalačných a konfiguračných služieb, ktoré zabezpečia vytvorenie a možnosť prevádzky bezpečnostného protokolu IEEE 802.1X v prostredí siete verejného obstarávateľa.

4 . Vykonanie segmentácie siete s ohľadom na súčasné prevádzkové požiadavky

Mesto Banská Bystrica má ambíciu vykonať segmentáciu siete v kontexte analýzy siete, ktorú bude nevyhnutné za týmto účelom vykonať. Obsahom tejto aktivity bude plánovanie segmentácie v kontexte identifikovaných možných logických segmentov s ohľadom na topológiu siete, prevádzkované agendové IS, výstupy realizovanej inventarizácie aktív a klasifikácie informácií a kategorizácie ako aj bezpečnostné požiadavky a požiadavky na výkonnosť. Predmetom dodávky bude vykonané mapovanie siete s cieľom získania komplexného a presného obrazu o existujúcej sieti Mesta vrátane všetkých relevantných informačných aktív.

V rámci realizovanej aktivity bude vykonané rozdelenie rozsahov IP adries v rámci vytváraných segmentov, pričom pre každé aktívum budú pridelené IP adresy z definovaných rozsahov. V rámci plnenia budú v kontexte novo dodávaných sieťových prvkov prehodnotené fyzické segmenty siete a z nich vychádzajúce logické segmenty pomocou VLAN. V rámci tejto aktivity sa vykoná konfigurácia dotknutých zariadení (switche, routre, firewally) tak, aby nastavenia zodpovedali schválenému návrhu segmentácie prevádzkou IKT Mesta. Súčasťou tejto aktivity zároveň bude vypracovanie komplexnej dokumentácie zachytávajúce celý stav vykonanej segmentácie, vrátane otestovania a overenia funkcionality.

Horeuvedené činnosti budú vykonávané v rozsahu siete v ktorej je aktívne využívaných 85 switchov, 40 routerov, 2 firewally vrátane zariadení, ktoré sú predmetom dodávky v rámci tohto projektu.

5. Výmena aktívnych prvkov CORE časti siete

V rámci tejto aktivity sa plánuje obstarať nové, nepoužité, v originálnom obale zabalené aktívne prvky CORE časti siete. Výmena sa plánuje s ohľadom na potrebu nahradenia end-of-sales and end-of-support aktívnych prvkov, doplnenie jestvujúcich ako aj s ohľadom na potrebu zabezpečenia väčšej bezpečnosti prevádzky siete ako aj prenosovej kapacity siete ako reakciou na neustále rastúce požiadavky na prenos v sieti Mesta. Od výmeny potrebných aktívnych prvkov CORE časti siete sa očakáva zároveň zabezpečiť kontinuitu požadovanej úrovne IT aktív ako aj primerané doby odozvy informačných aktív prevádzkovaných v sieti Mesta. Výmena aktívnych prvkov CORE časti siete je potrebná aj s ohľadom na zámer Mesta implementovať systém pre riadenie správy a prístupov koncových zariadení do siete Mesta a zámerom implementovať protokol IEEE 802.1X. Súčasný stav CORE časti siete neumožňuje

plnohodnotné nasadenie IEEE 802.1X v rozsahu očakávanej segmentácie siete zahŕňajúcej okrem nových CORE aktívnych prvkov aj obstarané aktívne prvky v rámci aktivity 3. tohto projektu. Mesto plánuje obstarať celkovo 9 ks aktívnych prvkov CORE časti siete. Súčasťou dodávky nových, nepoužitých zariadení zabalených v originálnom balení, bude ich inštalácia, konfigurácia a uvedenie do prevádzky tak, aby mohli dodávané zariadenia byť zahrnuté do výkonu segmentácie siete ako aj nasadenia overovania podľa IEEE 802.1X.

Súčasťou aktivity bude implementácia riešenia zberu prevádzkových údajov z dodaných zariadení typu Firewall.

6. Implementácia systému dvojfaktorovej autentifikácie pre vzdialený prístup do vnútornej siete

V rámci tejto aktivity sa očakáva implementovať riešenie pre vzdialený prístup do siete vrátane dodania a nasadenia mobilných SW ako aj HW tokenov a autentifikačného servera vyžadujúceho druhý stupeň overenia užívateľa prihlasujúceho sa do internej siete prostredníctvom implementácie služby 2-faktorového overovania („2FA“) pre celkovo 700 používateľov pristupujúcich do siete Mesta.

Navrhuje sa, aby implementovaný autentifikačný server od užívateľa vyžadoval zadanie mena a hesla a následne po úspešnom zadaní prihlasovacej kombinácie vyžiadal zadanie jednorazového hesla, ktoré bude možné užívateľom generovať prostredníctvom dodaného hardvérového a softvérového tokenu kompatibilného s mobilnými zariadeniami iOS, Android a Windows, čím sa zabezpečí ďalšia úroveň zabezpečenia prístupu do siete Mesta z vonkajšieho prostredia.

Súčasťou aktivity bude dodávka VPN klientov s bezpečnostným modelom s nulovou dôverou, teda VPN klient, ktorý zároveň disponuje funkcionalitou kontroly koncového zariadenia voči nastaveným prístupovým politikám. VPN klient bude zároveň disponovať funkcionalitou karantény pripájajúcich sa koncových zariadení a umožní izolovať napadnuté koncové zariadenia od zvyšku siete, čím sa minimalizuje ohrozenie internej siete z podozrivého zdroja.

7. Implementácia riešenia centrálneho bezpečnostného manažmentu pre koncové stanice

V rámci tejto aktivity sa plánuje implementovať ucelené riešenie prevencie a detekcie pred hrozbami z vonkajšieho prostredia. Riešenie bude zabezpečovať centrálnu správu ochrany koncových staníc, detekciu nevyžiadanej aktivity na koncových staniciach, funkcionalitu monitoringu prevádzky na koncových zariadeniach, skenovanie koncových zariadení ako aj funkcionalitu centrálneho nastavovania bezpečnostných pravidiel a politík pre koncové zariadenia. Riešenie umožní centrálne nastavovanie SW na koncových staniciach, nadobúdať informácie o telemetrii a prevádzke koncových staníc ako vykonávať reportovanie na úrovni koncových staníc.

Všetky aktivity vyššie budú podporované prierezovou aktivitou pozostávajúcou zo školení dotknutého personálu pre účely zachovania vysokej úrovne IB a KB ako aj kontinuity prevádzky informačných aktív Mesta.

Jednotlivé aktivity možno považovať za navzájom vecne, technicky, procesne súvisiace a ich realizácia bude nutná vo vzájomnom časovom priebehu, tak aby sa dosiahol maximálny efekt z ich súčasnej realizácie.

4. ARCHITEKTÚRA RIEŠENIA PROJEKTU

Predmetom projektu je predovšetkým nákup HW a SW prostriedkov, analytické činnosti sieťových špecialistov a špecialistov pre oblasť IB a KB. Zmena biznis architektúry, aplikačnej ako ani technologickej nebude realizovaná a aj aj vzhľadom na skutočnosť, že v predmetom projektu nie je plánované budovanie ISVS ako ani rozvoj žiadneho z jestvujúcich ISVS a ani migrácia do vládneho cloudu. Celkový prístup k architektúre ako aj popis sieťovej architektúry a jej logického zapojenia je popísaný bližšie kap. 5 dokumentu Projektový zámer. Mesto Banská Bystrica zároveň v tejto súvislosti uvádza a má za to, že nie je účelné uvádzať do verejne prístupného dokumentu ďalšie podrobnosti týkajúce sa infraštruktúry, na ktorej je prevádzkovaná základná služba ako aj ďalšie pre Mesto dôležité informačné aktíva, a z tohto dôvodu ďalšie, pre tento projekt nepožadované detaily, nesprístupňuje. Informácie v dokumente Projektový zámer sú zároveň uvedené v takej úrovni detailu, aby bolo orgánu vedenia jednoznačne možné verifikovať prioritné oblasti, do ktorých Mesto Banská Bystrica potrebuje realizovať nevyhnutné investície.

4.1 Biznis vrstva

Vzhľadom na charakter projektu – projekt z oblasti IB a KB je daná časť irelevantná.

4.2 Aplikačná vrstva

Vzhľadom na charakter projektu – projekt z oblasti IB a KB je daná časť irelevantná.

4.3 Dátová vrstva

Vzhľadom na charakter projektu – projekt z oblasti IB a KB je daná časť irelevantná.

4.4 Technologická vrstva

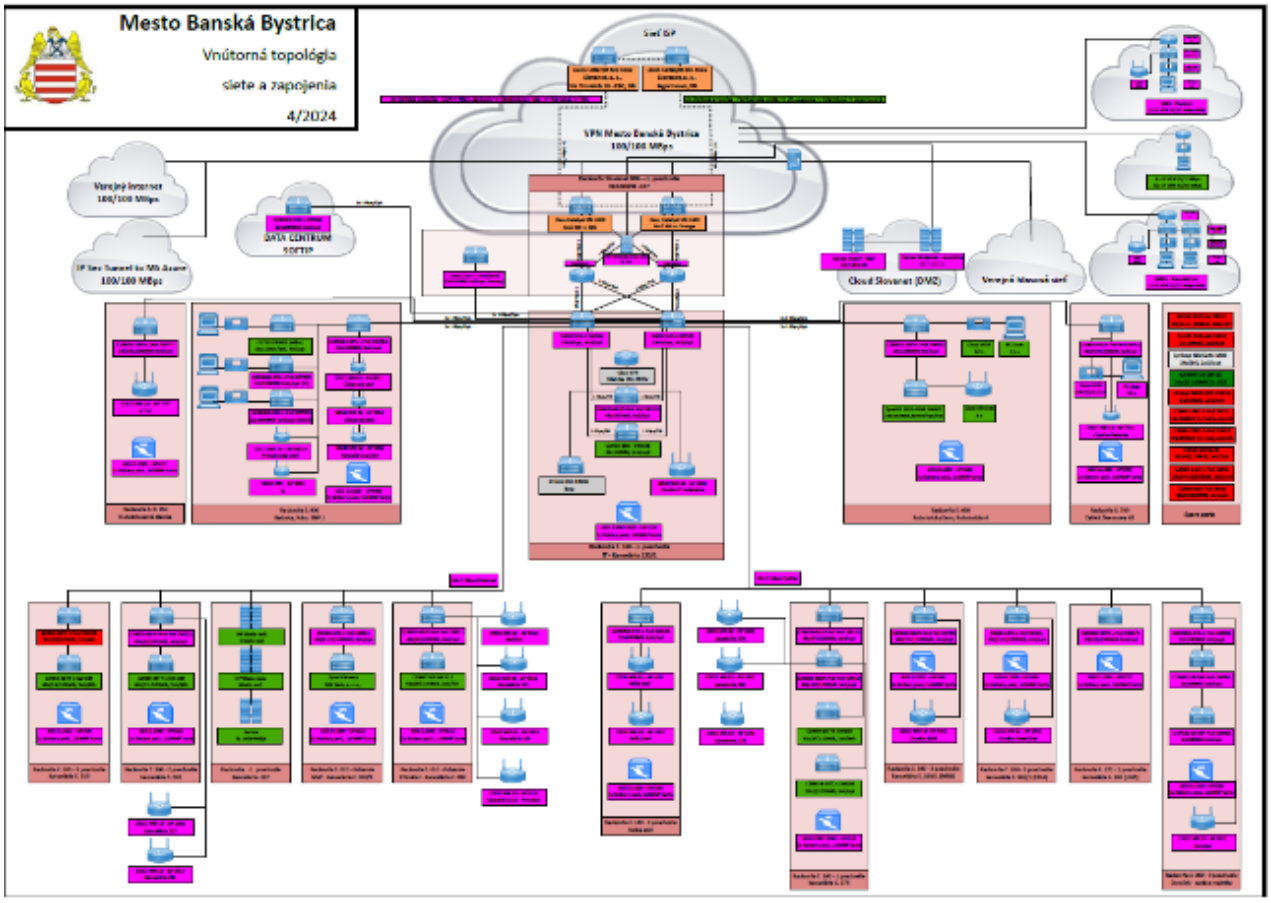
Súčasťou aktivít projektu je doplnenie jednotlivých HW položiek (firewally, router, switche) pre potreby obnovy jestvujúcej bezpečnostnej vrstvy. Položky, ktoré sa plánuje v rámci projektu nasadiť sú popísané vyššie v tomto dokumente ako aj v kap. 5 dokumentu Projektový zámer. Podrobná špecifikácia je obsiahnutá súčasne v rámci Výzvy na predkladanie indikatívnych cenových ponúk za účelom stanovenia predpokladanej nákladovosti hlavných aktivít projektu. Táto špecifikácia je zároveň v súlade s Katalógom požiadaviek, ktorý tvorí neoddeliteľnú súčasť dokumentácie k projektu.

4.4.1 Požiadavky na výkonnostné parametre, kapacitné požiadavky – TO BE

Parameter	Jednotky	Predpokladaná hodnota	Poznámka
Počet interných používateľov	Počet	250	Zamestnanci MsÚ
Počet súčasne pracujúcich interných používateľov v špičkovom zaťažení	Počet	700	Vrátane zamestnancov Mesta vrátane zamestnancov MsÚ
Počet externých používateľov (internet)	Počet	100 000	
Počet externých používateľov používajúcich systém v špičkovom zaťažení	Počet	125 000	
Počet transakcií (požiadavky na sieťový traffic)	Počet/obdobie	Viď Výzva Projektový zámer – špecifikácia HW	Požiadavky na aktívne sieťové prvky

4.4.2 Návrh riešenia technologickej / bezpečnostnej architektúry

Realizáciou aktivít projektu nedôjde k zmene topológie siete, ktorá v stave „AS-IS“ zodpovedá schéme nižšie:



4.4.3 Využívanie služieb z katalógu služieb vládneho cloudu

Vzhľadom na charakter projektu sa nebudú využívať žiadne služby vládneho cloudu.

5. ZÁVISLOSTI NA OSTATNÉ ISVS / PROJEKTY

Neevidujú sa žiadne závislosti na iné projekty alebo ISVS.

6. ZDROJOVÉ KÓDY

Vzhľadom na charakter projektu – projekt z oblasti IB a KB je daná časť irelevantná.

7. PREVÁDZKA A ÚDRŽBA

7.1 Prevádzkové požiadavky

Prevádzkové požiadavky budú pre navrhované riešenie rovnaké ako je ich súčasná úroveň:

Úrovne podpory používateľov:

Help Desk bude realizovaný cez 3 úrovne podpory s nasledovným označením:

L1 podpora riešenia (LEVEL 1, priamy kontakt používateľa) – zabezpečuje prevádzka IKT Mesta;

L2 podpora riešenia (LEVEL 2, postúpenie požiadaviek od L1) – vybraná skupina garantov so základnou znalosťou riešenia, zabezpečuje Help Desk prvej úrovne dodávateľa riešenia. Úroveň služieb, rozsah ako aj reakčné časy budú závislé od definovanej úrovne SLA zmluvy;

L3 podpory riešenia (LEVEL 3, postúpenie požiadaviek od L2) – vybraná skupina garantov s vysokou úrovňou špecializácie na v riešení použité technológie a postupy, rozsah ako aj reakčné časy budú závislé od definovanej úrovne SLA zmluvy.

Definícia:

Podpora L1 (podpora 1. stupňa) – začiatočná úroveň podpory, ktorá je zodpovedná za riešenie základných problémov a požiadaviek koncových používateľov a ďalšie služby vyžadujúce základnú úroveň technickej podpory. Základnou úlohou podpory 1. stupňa je zhromaždiť informácie, vykonať základnú analýzu a určiť príčinu problému a jeho klasifikáciu. Typicky sú v tejto úrovni riešené priamočiare a jednoduché problémy a základné diagnostiky, overenie dostupnosti jednotlivých vrstiev infraštruktúry (sieťové, operačné, vizualizačné, aplikačné a pod...) a základné užívateľské problémy (napr. zabudnutie hesla), overovanie nastavení SW a HW a pod.

Podpora L2 (podpora 2. stupňa) – riešiteľské tímy s hlbšou technologickou znalosťou akou disponuje L1. Riešitelia na úrovni podpory L2 komunikujú s L1 úrovňou a sú zodpovední za poskytovanie súčinnosti tejto úrovni. L2 úroveň zodpovedá za poskytovanie súčinnosti úrovni L1 v prípade, že L1 úroveň eskaluje na L2 úroveň svoju požiadavku. L2 úroveň zabezpečuje hlbšiu úroveň analýzy problému ako aj technickejší pohľad na riešenie problému. Výstupom kontroly na úrovni L2 môže byť potvrdenie, upresnenie alebo prehodnotenie hlásenia v závislosti na potrebách Mesta. Primárnym cieľom na úrovni L2 je dostať hlásenie čo najskôr pod kontrolu a následne ho adekvátne vyriešiť, prípadne neodkladne eskalovať problém na L3 úroveň.

Podpora L3 (podpora 3. stupňa) – predstavuje najvyššiu úroveň podpory pre riešenie najkomplexnejších a najkomplikovanejších incidentov/problémov, vrátane prevádzania hĺbkových analýz a riešenie extrémnych prípadov.

Očakávaná úroveň SLA:

Služby pre zamestnancov úradu: 24/7/365 s možnosťou nahlasovania prostredníctvom call centra a/alebo dedikovaného rozhrania help-desku s funkcionalitou ticketovacieho systému pre manažment incidentov ako aj meranie reakčných časov.

Riešenie incidentov – SLA parametre

Za incident je považovaná chyba v diele (riešení) t.j. správanie sa v rozpore s prevádzkovou a používateľskou dokumentáciou diela. Za incident nie je považovaná chyba, ktorá nastala mimo prostredia riešenia, napríklad výpadok el. energie, alebo vyššia moc, prípadne iná udalosť, ktorú nebolo možné dôvodným spôsobom predvídať.

Označovanie naliehavosti hlásených incidentov:

Označenie naliehavosti incidentu (kategória)	Závažnosť incidentu	Popis naliehavosti incidentu
A	**Kritická**	Je to vada spôsobená vážnou chybou a/alebo nedostatkom dodávaného riešenia, pričom táto chyba a/alebo nedostatok zabraňuje používaniu dodávaného riešenia. Nie je možné poskytnúť požadovaný výstup z riešenia.
B	**Vysoká**	Je vada, spôsobená chybou a/alebo nedostatkom dodávaného riešenia, pričom táto chyba a/alebo nedostatok obmedzuje používanie dodávaného riešenia nasledovne: Niektoré funkcie (moduly, komponenty, objekty, programy) dodávaného riešenia nie sú funkčné alebo nie je umožnený prístup k niektorej funkcii (modulu, komponentu, objektu, programu) dodávanej dodávaného riešenia.
C	**Stredná**	Do tejto kategórie spadajú všetky chyby a/alebo nedostatky spojené s používaním dodávaného riešenia, ktoré nie sú klasifikované ako závažné alebo kritické vady, pričom však čiastočne obmedzujú používanie dodávaného riešenia. Nastavenie parametrov systému Poskytovateľom alebo (ii) Vzniknutá vada a/alebo nedostatok má za príčinu miernu nepohodlnosť pri práci s dodávaným riešením, ktorá je však funkčná.

Úroveň možného dopadu

Označenie závažnosti incidentu	Dopad	Popis dopadu
1	**Katastrofický**	Katastrofický dopad, priamy finančný dopad alebo strata dát (napr. znefunkčnenie základnej služby v celom jej rozsahu).
2	**Značný**	Značný dopad alebo strata dát (napr. znefunkčnenie základnej služby v jej podstatnom rozsahu).
3	**Malý**	Malý dopad alebo strata dát (ostatné udalosti nespadajúce do kategórie značný alebo katastrofický).

Výpočet priority incidentu je kombináciou dopadu a naliehavosti v súlade s best practices ITIL V3 uvedený v nasledovnej matici:

Označenie priority incidentu	Reakčná doba[(1)] od nahlásenia incidentu po začiatok riešenia incidentu	Doba konečného vyriešenia incidentu od nahlásenia incidentu (DKVI)[(2)]	Spoľahlivosť [(3)] (počet incidentov za mesiac)
1	**0,5 hod.**	4 hodín	1
2	**1 hod.**	12 hodín	2
3	**1 hod.**	24 hodín	10
4	**1 hod.**	Vyriešené a nasadené v rámci plánovaných releasov	

(1) Reakčná doba je čas medzi nahlásením incidentu Mestom Banská Bystrica (vrátane užívateľov riešenia, ktorí nie sú v pracovnoprávnom vzťahu s Mestom) na helpdesk úrovne L2 a jeho prevzatím na riešenie.

(2) DKVI znamená obnovenie štandardnej prevádzky - čas medzi nahlásením incidentu Mestom Banská Bystrica a vyriešením incidentu úspešným uchádzačom (do doby, kedy je funkčnosť prostredia znovu obnovená v plnom rozsahu). Doba konečného vyriešenia incidentu od nahlásenia incidentu Mestom Banská Bystrica (DKVI) sa počíta počas celého dňa. Do tejto doby sa nezarátava čas potrebný na nevyhnutnú súčinnosť Mesta Banská Bystrica, ak je potrebná pre vyriešenie incidentu. V prípade potreby je úspešný uchádzač oprávnený požadovať od Mesta Banská Bystrica schválenie riešenia incidentu.

(3) Maximálny počet incidentov za kalendárny mesiac. Každá ďalšia chyba nad stanovený limit spoľahlivosti sa počíta ako začatý deň omeškania bez odstránenia vady alebo incidentu. Duplicitné alebo technicky súvisiace incidenty (zadané v rámci jedného pracovného dňa, počas pracovného času 8 hodín) sú považované ako jeden incident.

4) Incidenty nahlásené Mestom Banská Bystrica úspešnému uchádzačovi:

a. Majú prioritu 3 a nižšiu;

7.2 Požadovaná dostupnosť IS:

Popis	Parameter	Poznámka
Prevádzkové hodiny	8 hodín	od 8:00 hod. - do 16:00 hod. počas pracovných dní
Servisné okno	10 hodín	od 19:00 hod. - do 5:00 hod. počas pracovných dní
	24 hodín	od 00:00 hod. - 23:59 hod. počas dní pracovného pokoja a štátnych sviatkov Servis a údržba sa bude realizovať mimo pracovného času.
Dostupnosť produkčného prostredia IS	99,90 %	98,5% z 24/7/365 t.j. max ročný výpadok je 66 hod. Maximálny mesačný výpadok je 5,5 hodiny. Vždy sa za takúto dobu považuje čas od 0.00 hod. do 23.59 hod. počas pracovných dní v týždni. Nedostupnosť IS sa počíta od nahlásenia incidentu Zákazníkom v čase dostupnosti podpory Poskytovateľa (t.j. nahlásenie incidentu na L3 v čase od 6:00 hod. - do 18:00 hod. počas pracovných dní). Do dostupnosti IS nie sú započítavané servisné okná a plánované odstávky IS. V prípade nedodržania dostupnosti IS bude každý ďalší začatý pracovný deň nedostupnosti braný ako deň omeškania bez odstránenia vady alebo incidentu.

7.2.1 Dostupnosť (Availability)

Dostupnosť znamená, že riešenie ako výstup projektu je prístupné v okamihu jeho potreby. Narušenie dostupnosti sa označuje ako nežiaduce zničenie (destruction) alebo nedostupnosť. Dostupnosť je zvyčajne vyjadrená ako percento času v danom období, obvykle za rok. V projekte sa uvažuje 99,90 % dostupnosť.

7.2.2 RTO (Recovery Time Objective)

V rámci projektu sa očakáva obnova po výpadku do 4 hodín resp. v závislosti od závažnosti identifikovaného problému.

7.2.3 RPO (Recovery Point Objective)

Projekt nerieši zálohovanie dát – výpadok riešenia nebude mať dopad na jestvujúce ISVS a ich zálohovanie dát.

8. POŽIADAVKY NA PERSONÁL

Projekt sa bude riadiť v súlade s platnou legislatívou v oblasti riadenia projektov IT. Pre potreby riadenia projektu bude vytvorený riadiaci výbor projektu a budú menovaní členovia Riadiaceho výboru projektu (ďalej len „RV“), projektový manažér a členovia projektového tímu.

Riadiaci výbor projektu tvoria minimálne 3 členovia, vrátane predsedu Riadiaceho výboru.
Riadiaci výbor (RV), v minimálnom zložení:

- predseda riadiaceho výboru;
- zástupca kľúčových používateľov objednávateľa;
- zástupca dodávateľa (doplní sa až po VO).

Riadiaci výbor je riadený predsedom, ktorým je zástupca Mesta Banská Bystrica. V prípade neprítomnosti predsedu na zasadnutí Riadiaceho výboru, predseda musí na toto konkrétne zasadnutie písomne delegovať svoju funkciu v rozsahu svojich práv a povinností formou splnomocnenia na zástupcu, ktorým môže byť aj iný člen Riadiaceho výboru s hlasovacím právom, prípadne iná splnomocnená osoba.

Riadiaci výbor zasadá pravidelne, najmenej jedenkrát za dva (2) po sebe nasledujúce kalendárne mesiace. Zasadnutie Riadiaceho výboru zvoláva predseda. Zasadnutie Riadiaceho výboru vedie predseda, prípadne ním určený zástupca, na ktorého predseda na dané zasadnutie písomne delegoval svoju funkciu, alebo ten člen Riadiaceho výboru, ktorý požiadal o zasadnutie Riadiaceho výboru.

Hlavné dokumenty spojené s činnosťou Riadiaceho výboru sú program zasadnutia, pracovný materiál a záznam zo zasadnutia Riadiaceho výboru, ktorého prílohou musí byť aj prezenčná listina, prípadne aj písomné splnomocnenia členov Riadiaceho výboru. Závery zo zasadnutia Riadiaceho výboru a jednotlivé body zo zasadnutia Riadiaceho výboru sa prijímajú súhlasným hlasovaním nadpolovičnej väčšiny prítomných členov Riadiaceho výboru s hlasovacím právom. Hlas predsedu má v prípade rovnosti hlasov hodnotu dvoch hlasov.

Každý člen Riadiaceho výboru ma tieto práva a povinnosti:

a. právo a povinnosť zúčastňovať sa na zasadnutiach Riadiaceho výboru;
b. právo uplatniť si pripomienky, podávať podnety alebo vyjadriť sa k pracovnému materiálu predloženému na zasadnutí Riadiaceho výboru alebo v rámci dištančného hlasovania, ak sa jedná o člena Riadiaceho výboru s hlasovacím právom,
c. právo podávať návrhy a podnety týkajúce sa činnosti Riadiaceho výboru,
d. právo nahliadať do projektovej dokumentácie,
e. navrhovať zmeny Štatútu,
f. iné práva v zmysle tohto Štatútu a Projektového iniciálneho dokumentu (PID).

Člen Riadiaceho výboru zachováva mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvedel pri výkone svojej funkcie alebo v súvislosti s ňou a ktoré v záujme Riadiaceho výboru nemožno oznamovať tretím osobám, a to aj po ukončení realizácie projektu. Riadiaci výbor sa zriaďuje na účely realizácie projektu a bude zostavený v zložení:

ID	Meno a Priezvisko	Pozícia	Subjekt
1.	TBD	Predseda RV	Mesto Banská Bystrica
3.	TBD	Kľúčový používateľ	Mesto Banská Bystrica
7.	TBD	Zástupca Zhotoviteľa	TBD

Podrobná štruktúra RVP bude definovaná v rámci projektového iniciálneho dokumentu („PID“) v súlade s metodikou riadenia projektov PRINCE2®.

Projektový tím

Riadenie projektu zo strany Objednávateľa bude zabezpečené prostredníctvom Projektového manažéra a Finančného manažéra a bude trvať počas celej doby realizácie projektu. Bude pokrývať oblasť projektového riadenia (projektový manažment, celková koordinácia projektu, celkový dohľad nad dodávkou dodávaného Diela, vrátane kvality), finančného riadenia a monitorovania realizácie projektu v zmysle riadenia podľa Vyhlášky č. 401/2022 Z. z. v platnom znení.

Projektový tím bude pozostávať z pozícií:

Povinné projektové role:

- Projektový manažér objednávateľa;
- Kľúčový používateľ;
- IT architekt;
- Vlastník procesov;
- Manažér kybernetickej a informačnej bezpečnosti;
- Projektový manažér zhotoviteľa;
- Špecialista pre bezpečnosť IT;
- IT analytik;
- Špecialista pre infraštruktúrny/HW špecialista;
- IT/IS konzultant;
- IT tester;
- Školiteľ pre IT systémy.
- iii) Ďalšie projektové role:
- Finančný manažér,

Projektový manažér Objednávateľa bude zabezpečovať koordináciu projektových činností a manažment v súlade s metodikou

PRINCE2 (hlavné dokumenty, priebežné manažérske výstupy, a pod.). Projektový manažér Objednávateľa bude riadiť, administratívne a organizačne zabezpečovať implementáciu projektu, komunikovať s dodávateľmi, sledovať plnenie harmonogramu projektu a zabezpečovať dokumenty požadované MIRRI. Zároveň bude v spolupráci s projektovým manažérom dodávateľa koordinovať realizáciu hlavných aktivít, činností a úloh projektu. Zodpovednosťou projektového manažéra je v spolupráci s finančným manažérom (objednávateľa) finančné riadenie projektu kontrolu rozpočtu projektu a jeho súlad s účtovnými dokladmi. Kontrolu podpornej účtovnej dokumentácie a poradenstvo pri definovaní oprávnených výdavkov bude zabezpečovať finančný manažér Objednávateľa.

Súčasťou projektovej kancelárie a projektového riadenia bude tiež operatívna projektová podpora zabezpečujúca administratívnu podporu pre písomnú komunikáciu, administratívne vedenie projektovej dokumentácie a prípravu podkladov pre členov projektového tímu, organizáciu stretnutí a pod.. V rámci aktivity budú taktiež zabezpečovaný manažment a hodnotenie kvality zo strany Objednávateľa.

ID	Meno a Priezvisko	Pozícia	Organizačný útvar	Rola v projekte
1.	TBD	TBD	TBD	Projektový manažér
2.	TBD	TBD	TBD	Kľúčový používateľ
3.	TBD	TBD	TBD	IT architekt
4.	TBD	TBD	TBD	Vlastník procesov
5.	Ing. Bibiána Palušková	Manažér IB a KB	PR-MKB	Manažér kybernetickej a informačnej bezpečnosti
6.	TBD	TBD	TBD	Projektový manažér zhotoviteľa
7.	TBD	TBD	TBD	Špecialista pre bezpečnosť IT
8.	TBD	TBD	TBD	IT analytik
9.	TBD	TBD	TBD	Manažér kvality
10.	TBD	TBD	TBD	IT/IS konzultant
11.	TBD	TBD	TBD	IT tester
12.	TBD	TBD	TBD	Školiteľ pre IT systémy
13.	TBD	TBD	TBD	Finančný manažér

9. IMPLEMENTÁCIA A PREBERANIE VÝSTUPOV PROJEKTU

Projekt bude v zmysle Vyhlášky 401/2023 Z.z. o riadení projektov a zmenových požiadaviek riadený a realizovaný spôsobom waterfall. Projekt bude vzhľadom na previazanosť jednotlivých aktivít realizovaný v rámci jedného samostatného inkrementu.

10. PRÍLOHY

Dokument neobsahuje žiadne prílohy.