projekt_2800_Pristup_k_projektu_detailny

PRÍSTUP K PROJEKTU

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

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

Schvaľovanie dokumentu

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

1. História dokumentu

Verzia	Dátum	Zmeny	Meno
0.01	19.06.2024	prvá verzia dokumentu	Denis Dojčan
0.02	21.06.2024	druha verzia dokumentu	Denis Dojčan
1.00	24.06.2024	zapracovanie pripomienok a súladu s vyhláškou č. 401/2023 Z. z., finálna verzia v súlade so ŽoNFP	Denis Dojčan

2. Účel dokumentu

V súlade s Vyhláškou MIRRI SR **č. 401/2023 Z. z. o riadení projektov a zmenových požiadaviek v prevádzke IT VS** je dokument Prístup k projektu určený na rozpracovanie detailných informácií prípravy projektu z pohľadu aktuálneho stavu, budúceho stavu a navrhovaného riešenia.

Dokument Prístup k projektu v zmysle vyššie uvedenej vyhlášky obsahuje opis navrhovaného riešenia, architektúru riešenia projektu na úrovni biznis vrstvy, aplikačnej vrstvy, dátovej vrstvy, technologickej vrstvy, infraštruktúry navrhovaného riešenia, bezpečnostnej architektúry, špecifikáciu údajov spracovaných v projekte, čistenie údajov, prevádzku a údržbu výstupov projektu, prevádzkové požiadavky, požiadavky na zdrojové kódy. Dodávané riešenie bude v súlade so zákonom. Zároveň opisuje aj implementáciu projektu a preberanie výstupov projektu.

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

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

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

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

2.1 Použité skratky a pojmy

Z hľadiska formálneho sú použité pojmy v rámci celého dokumentu definované priebežne, štandardne pri prvom použití v zátvorke označením („*ďalej len*“).

SKRATKA/POJEM	POPIS
KIB	kybernetická a informačná bezpečnosť
MIRRI	Ministerstvo investícií, regionálneho rozvoja a informatizácie
SR	Slovenská republika
IT	informačné technológie
VS	verejná správa
NFP	nenávratný finančný príspevok
KB	kybernetická bezpečnosť
ITVS	informačné technológie verejnej správy
OPII	Operačný program Integrovaná infraštruktúra
EFRR	Európsky fond regionálneho rozvoja
IB	informačná bezpečnosť
TT	Trnava
RÚVZ	Regionálny úrad verejného zdravotníctva so sídlom v Trnave
PN	Piešťany
HC	Hlohovec
TTSK	Trnavský samosprávny kraj
MZ	Ministerstvo zdravotníctva
NR	Národnej rady
ISVS	informačných systémov verejnej správy
MU	merateľné ukazovatele
MJ	merná jednotka
NBÚ	Národný bezpečnostný úrad
IKT	informačno-komunikačné technológie
NKIVS	Národná koncepcia informatizácie verejnej správy
HW	hardvér
SW	softvér
RV	Riadiaci výbor
MJ	merná jednotka

JC	jednotková cena
NFP	nenávratný finančný príspevok
VO	verejné obstarávanie
HK	hodnotiace kritérium
KPI	výkonnostný ukazovateľ
ŽoNFP	Žiadosť o nenávratný finančný príspevok

2.2 Konvencie pre typy požiadaviek

Hlavné kategórie požiadaviek v zmysle katalógu požiadaviek, rozdeľujeme na funkčné, nefunkčné a technické.

V rámci projektu budú definované tri základné typy požiadaviek:

Funkcionálne (používateľské) požiadavky majú nasledovnú konvenciu:

FRxx

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

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

NRxx

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

Tabuľka 1 Hlavné kategórie požiadaviek v zmysle katalógu požiadaviek

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

3. Popis navrhovaného riešenia

Obsahom tejto kapitoly je manažérsky sumár navrhovaného riešenia z pohľadu architektúry.

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

- Analýza aktuálneho stavu.
- Naplnenie technických, organizačných a procesných podmienok.

- Naplnenie personálnych podmienok na zabezpečenie riadneho chodu RÚVZ so sídlom v Trnave.
- Technologické zabezpečenie.

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

Implementácia projektu bude pozostávať z nasledovných aktivít:

A1: Analýza a Dizajn

1.1 Konzultačné a analytické práce

1.2 Identifikácia možností realizácie, potrebných zdrojov a riešení

1.3 Identifikácia a analýza rolí, procesov a integrácií

1.4 Funkčná a nefunkčná špecifikácia celého riešenia

1.5 Definícia všetkých bezpečnostných a špecializovaných produktov spolu s akceptačnými kritériami

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

Výstupom bude:

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

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

A2: Obstaranie HW/SW/OS:

2.1 Nákup HW a SW rozširujúceho funkcionalitu existujúceho IS

2.2 Nákup HW a SW Deduplikačné zálohovacie úložisko

Výstupom bude:

- Obstaraný HW a SW (licencie)

A3: Implementácia a Testovanie

3.1 Zavedenie a konfigurácia zariadení a integrácia do siete úradu.

3.2 Integrácia MIS - registratúry s novou konfiguráciou na sieti.

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

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

3.5 Obvyklé testovanie a ladenie riešení popri ich implementácii.

3.6 Konfigurácia segmentácie, testovanie a ladenie riešenia.

3.7 Testovanie funkcionality riešenia.

3.8 Testovanie zraniteľností a „case-hardening“.

3.9 Testovanie integrácií.

3.10 Testovanie pilotnej prevádzky.

3.11 Akceptačné testovanie.

Výstupom bude:

- Akceptačný protokol

A4: Nasadenie a monitorovanie:

4.1 Nasadenie riešenia do produkčného prostredia.

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

4.3 Prechod na plnú prevádzku.

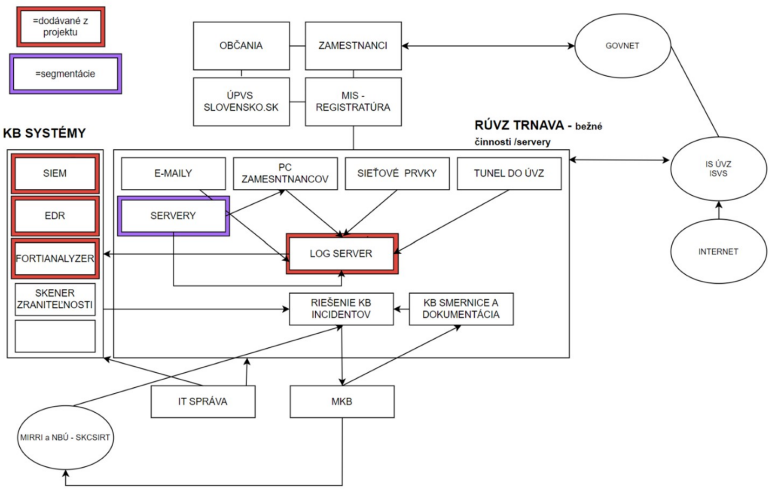
Výstupom bude:

- Akceptačný protokol

5 - Podpora prevádzky (SLA)

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

4. Architektúra riešenia projektu



4.1 Biznis vrstva

n/a

4.2 Aplikačná vrstva

n/a

4.3 Dátová vrstva

n/a

4.4 Technologická vrstva

1) Segmentácia siete + HW

Segmentácie LAN sieťovej vrstvy ako architektonického prístupu, ktorý rozdeľuje sieť na viacero segmentov alebo podsietí, z ktorých každá funguje ako samostatná sieť. To umožňuje správcom siete riadiť tok prevádzky medzi podsieťami na základe podrobných pravidiel. Segmentácia prinesie zlepšenie monitorovania, zvýšenie výkonu, lokalizáciu technických problémov a čo je najdôležitejšie, zvýšenie bezpečnosti. Vďaka segmentácii siete je možné neoprávneným používateľom alebo priamo útočníkom zabrániť v získaní prístupu k hodnotným aktivitám či informáciám. Súčasťou segmentácie LAN sieťovej vrstvy je aj zabezpečenie ochrany perimetra ako vstupnej brány firewall do organizácie, ktorá zabezpečí monitorovanie a filtrovanie prichádzajúcej či odchádzajúcej sieťovej prevádzky na základe vopred stanovených bezpečnostných zásad organizácie.

Segmentácia LAN sieťovej vrstvy prinesie:

- Zabezpečenie siete prostredníctvom firewall brány, ktorá poskytuje kontrolu komunikácie na aplikačnej úrovni, hĺbkovej kontroly paketov (DPI), systém prevencie nevhodných aktivít (IPS) a ďalších bezpečnostných funkcionalít.
- Rozdelenie siete na viacero segmentov alebo podsietí zabezpečujúcich lepšie monitorovanie, zaznamenávanie udalostí a správu siete prostredníctvo
- Nastavenie bezpečnostných pravidiel medzi jednotlivými podsieťami kvôli zabráneniu získania prístupu.
- Filtrovanie prístupu medzi jednotlivými segmentami siete.
- Zvýšenie bezpečnosti prenášaných dát či kontrola siete, povolenie používateľom prístup iba k určitým sieťovým zdrojom.
- Zvýšenie výkonu pri sieti s menším počtom hostiteľov. Lokálna prevádzka je minimalizovaná.

2) Implementácia nástroja na sledovanie a detekciu prevádzky a neoprávnených spojení na hranici s vonkajšou sieťou

Nástroj na sledovanie a detekciu prevádzky je výkonná platforma na správu logov, analýzu a reportovanie, ktorá poskytuje organizáciám orchestráciu, automatizáciu a reakciu z jedného miesta pre zjednodušené bezpečnostné operácie, proaktívnu identifikáciu a nápravu rizík a kompletnú viditeľnosť celého povrchu útoku.

Tento nástroj, integrovaný s bezpečnostnou infraštruktúrou, poskytuje pokročilé schopnosti detekcie hrozieb, centralizovanú bezpečnostnú analýzu a úplnú informovanosť a kontrolu nad bezpečnostným postojom, čo pomáha bezpečnostným tímom identifikovať a eliminovať hrozby skôr, ako dôjde k narušeniu.

Orchestruje bezpečnostné nástroje, ľudí a procesy pre zjednodušené vykonávanie úloh a pracovných postupov, analýzu a reakciu na incidenty a rýchle urýchlenie detekcie hrozieb, tvorby prípadov a vyšetrovania, ako aj zmiernenie a reakciu.

Automatizuje pracovné postupy a spúšťajte akcie pomocou konektorov, playbookov a obslužných programov na urýchlenie schopnosti vášho tímu reagovať na kritické upozornenia a udalosti, ako aj SLA pre reguláciu a dodržiavanie predpisov.

Reaguje v reálnom čase na útoky na sieťovú bezpečnosť, zraniteľnosti a varovania o potenciálnych kompromitáciách s využitím informácií o hrozbách, korelácie udalostí, monitorovania, upozornení a reportovania pre okamžitú taktickú reakciu a nápravu.

3) Implementácia centralizovaného systému ochrany pred škodlivým kódom s monitorovaním detekcie inštalácie nelegálneho obsahu, vrátane automatizovaných nástrojov na detekciu škodlivej komunikácie na koncových staniciach a serveroch.

Implementácia a konfigurácia EDR riešenia na všetky existujúce koncové stanice a servery vrátane správy administrácie nasadeného systému. Produkt musí poskytovať detekciu hrozieb v reálnom čase na koncových zariadeniach s využitím viacvrstvových metód vrátane analýzy správania, signatúr a strojového učenia, a poskytovať automatickú prevenciu proti známym a neznámym hrozbám bez zásahu používateľa. Automatizovaná reakcia na bezpečnostné incidenty musí zahŕňať blokovanie, karanténu a odstránenie hrozieb, pričom administrátori musia mať možnosť manuálne reagovať prostredníctvom centralizovaného rozhrania. Produkt musí poskytovať kontinuálne monitorovanie stavu a aktivity koncových zariadení, pokročilú analýzu hrozieb vrátane forenznej analýzy a retrospektívneho vyhľadávania, a umožňovať vizualizáciu útokov a šírenia hrozieb v rámci siete. Integrácia s ďalšími bezpečnostnými riešeniami, podpora štandardných protokolov a API pre interoperabilitu a kompatibilita s rôznymi operačnými systémami vrátane Windows, macOS a Linux sú nevyhnutné. Produkt musí zabezpečovať šifrovanie dát pri prenose aj v kľudovom stave, byť v súlade s relevantnými právnymi a regulačnými požiadavkami na ochranu súkromia, a poskytovať nástroje na správu a kontrolu prístupu k citlivým údajom. Intuitívne a ľahko použiteľné rozhranie pre administrátorov a bezpečnostných špecialistov, prispôsobenie dashboardov a reportov, real-time notifikácie a upozornenia na bezpečnostné incidenty sú kľúčové. Produkt musí byť škálovateľný na podporu rastúceho počtu koncových zariadení a objemu dát, optimalizovaný pre rýchle spracovanie bezpečnostných udalostí a analýz, a zabezpečiť minimálnu odozvu a vysokú dostupnosť služieb.

4) Bezpečnostné zálohovacieho úložisko

Bezpečnostné zálohovacieho úložisko zabezpečí možnosť realizácie zálohovania údajov v zabezpečenej podobe ukladania záloh a ich následnej rýchlej a spoľahlivej obnovy s kontrolou ochrany pred škodlivým kódom.

Bezpečnostné zálohovacie úložisko prístupov prinesie:

- Deduplikáciu dát prostredníctvom pokročilých algoritmov, ktoré identifikujú a eliminujú redundantné dáta ešte pred ich uložením. To umožňuje výrazne znížiť množstvo úložného priestoru potrebného pre zálohy. Proces deduplikácie prebieha v reálnom čase, čo eliminuje potrebu dodatočného spracovania dát a zvyšuje celkový výkon systému.

- Šifrovanie dát, ktoré zabezpečí ochranu citlivých informácií pred neoprávneným prístupom počas prenosu aj uloženia záloh.
- Kontrolu integrity záloh.
- Centralizovanú správu zálohovacieho úložiska.

4.5 Bezpečnostná architektúra

Popis TO BE stavu riešenia bezpečnostnej architektúry

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

Zdôvodnenie

- Zachovanie pôvodného stavu nie je riešením z dôvodu nedostatku úrovne kybernetickej bezpečnosti a aktuálne i nespĺňania povinností vyplývajúcich zo Z. z. 69/2018 a Vyhlášky NBÚ.
- Migrovanie registratúry do siete ÚVZ nie je možné z dôvodu rýchlosti linky, keďže všetky úrady sú sieťovo prepojené a v iných lokalitách a pristupovanie všetkých úradov by ovplyvnilo rýchlosť linky a efektivitu práce.
- Zanechanie registratúry a zvýšenie úrovne kybernetickej bezpečnosti a splnenie povinností vyplývajúcich zo Z. z. 69/2

Súlad navrhovanej bezpečnostnej architektúry s dotknutými právnymi normami a s technickými normami

Projekt nevyžaduje zmeny legislatívy.

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

- Zákon 69/2018 Z.z. (NBÚ) o KB (od 30.1.2018),
- Zákon 95/2019 Z.z. o IT VS (od 27.3.2019),
- Zákon 576/2004 Z.z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov
- Zákon 355/ 2007 o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov
- Vyhláška č.78/2020 Z.z. o štandardoch pre ITVS (od 1.5.2020),
- Vyhláška č.85/2020 Z.z. o riadení projektov (od 1.5.2020 do 14.11.2023),
- Vyhláška č.401/2023 Z.z. o riadení projektov a zmenových požiadaviek v prevádzke IT VS (od 15.11.2023),
- Vyhláška 179/2020 Z.z. o obsahu bezpečnostných opatrení IT VS (od 30.6.2020),
- Vyhláška 362/2018 Z.z. o obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (od 11.12.2018),
- Vyhláška 547/2021 Z.z. (UX/IDSK) o elektronizácii agendy VS (od 1.1.2022).

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

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

paragraf 80

Povinnosti zdravotníckeho pracovníka

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

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

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

(5) Povinná mlčanlivosť sa neporuší ani informovaním

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

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

Zákon 576 z 21. októbra 2004

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

paragraf 24

Poskytovanie údajov zo zdravotnej dokumentácie

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

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

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

paragraf 25

Sprístupňovanie údajov zo zdravotnej dokumentácie

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

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

5. Závislosti na ostatné ISVS / projekty

Projekt nemá závislosti na iný projekt.

6. Zdrojové kódy

n/a

7. Prevádzka a údržba

n/a – bude riešená interným IT, nie SLA

7.1 Požadovaná dostupnosť IS:

V nasledujúcej tabuľke je uvedená dostupnosť IS:

Tabuľka 2 Dostupnosť IS

Popis	Parameter	Poznámka

Prevádzkové hodiny	12 hodín	od 6:00 hod. - do 18:00 hod. počas pracovných dní
Servisné okno	8 hodín	od 6:00 hod. - do 18:00 hod. počas pracovných dní
Dostupnosť produkčného prostredia IS	98,5%	98,5% z 24/7/365 t.j. max ročný výpadok je 66 hod.

7.2 RTO (Recovery Time Objective)

24 hodín

7.3 RPO (Recovery Point Objective)

24 hodín

8. Požiadavky na personál

Požiadavky na projektové personálne zabezpečenie (projektové role a ich obsadenie)

Detailný popis sa nachádza v kapitole **9 Projektový tím** z dokumentu „PROJEKTOVY_ZAMER“.

Rámcové požiadavky na obsadenie TO BE procesu

n/a

Požiadavky potrebných školení a certifikátov

n/a

9. Implementácia a preberanie výstupov projektu

Projekt bude realizovaný metódou Waterfall

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

Dokumenty obsahujúce informácie klasifikované ako chránené a prísne chránené podľa Vyhlášky č.362/2018 Z.z, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení budú v rámci projektu odovzdávané v elektronickej podobe šifrované pomocou PGP kľúčov, ktoré si MF SR a dodávateľ na začiatku projektu vymenia.

Projekt bude riadený na základe princípu **WATERFALL – VODOPÁDOVÝ PRÍSTUP** – vychádza to zo samotnej povahy projektu a princípu migrácie.

Pri akceptácii budú vyhotovované vopred definované akceptačné kritériá a požiadavky z katalógu funkčných a nefunkčných požiadaviek vzťahujúce sa k jednotlivých miľníkom projektu.

Akceptačný protokol bude schválený Riadiacim výborom na základe schválených akceptačných kritérií a požiadaviek z katalógu požiadaviek a bude podkladom ku fakturácii.

10. Odkazy

Odkaz na projekt a príslušnú dokumentáciu v META IS: projekt_2800_Pristup_k_projektu_detailny