**PRÍSTUP K PROJEKTU**

**Vzor pre manažérsky výstup I-03**

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

|  |  |
| --- | --- |
| Povinná osoba | Úrad vlády Slovenskej republiky |
| Názov projektu | Zvýšenie úrovne kybernetickej a informačnej bezpečnosti Úradu vlády Slovenskej republiky 2.0 |
| Zodpovedná osoba za projekt | Mgr. Miloš Gallovič |
| Realizátor projektu | Úrad vlády Slovenskej republiky |
| Vlastník projektu | Ing. Branislav Világi |

**Schvaľovanie dokumentu**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Položka | Meno a priezvisko | Organizácia | Pracovná pozícia | Dátum | Podpis  (alebo elektronický súhlas) |
| Vypracoval | Mgr. Miloš Gallovič | Úrad vlády Slovenskej republiky |  | 07.10.2024 |  |

# História dokumentu

|  |  |  |  |
| --- | --- | --- | --- |
| Verzia | Dátum | Zmeny | Meno |
| 0.1 | 01.10.2024 | Pracovný návrh | Mgr. Miloš Gallovič |
| 1.0 | 07.10.2024 | Final pre podanie na hodnotenie | Mgr. Miloš Gallovič |

# Účel dokumentu

V súlade s Vyhláškou č. 401/2023 Z.z. je dokument I-03 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 musí byť v súlade so zákonom. Zároveň opisuje aj implementáciu projektu a preberanie výstupov projektu.

## Použité skratky a pojmy

|  |  |  |
| --- | --- | --- |
| **ID** | **SKRATKA** | **POPIS** |
| 1. | API | Application programming interface |
| 2. | BPMN | Business Process Model and Notation |
| 3. | CSRÚ | Centrálna správa referenčných údajov |
| 4. | DevOps | Je skrátený názov pre developer, security alebo aj automatizovaný devops ako súbor procesov medzi vývojom a prevádzkou, skratka z developer operations. Vysvetlenie detail viď <https://en.wikipedia.org/wiki/DevOps> |
| 5. | DMS | Document management system |
| 6. | EDR | Endpoint Detection and Response |
| 7. | EÚ | Európska únia |
| 8.. | HW | Hardware |
| 9. | HLD | High level dizajn – vysokoúrovňový dizajn napr architektúru, bezpečnosť |
| 10. | IaaS | Infrastructure as a service |
| 11. | IAM | Identity and Access Management |
| 12. | IKT | Informačno-komunikačné technológie |
| 13. | IS | Informačný systém |
| 14. | IS VS | Informačný systém verejnej správy |
| 15. | KPI | Key performance indicator – Kľúčové indikátory, prostredníctvom ktorých sa meria naplnenie cieľov projektu. |
| 16. | LLD | Low level dizajn – nízkoúrovňový dizajn napr. pre architektúru, bezpečnosť. Obsahuje detailné dizajny až na úrovní nastavení parametrov |
| 17. | MDM | Mobile devicemanagement |
| 18. | MIRRI | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky |
| 19. | MV SR | Ministerstvo vnútra SR |
| 20. | NKIVS | Národná koncepcia informatizácie verejnej správy |
| 21. | OOÚ | Ochrana osobných údajov |
| 22. | PO | Plán obnovy a odolnosti |
| 23. | OVM | Orgán verejnej moci |
| 24. | PaaS | Platform as a service |
| 25. | PILOT | PILOT - Prevádzka riešenia na vybraných aktéroch na produkčnom prostredí. |
| 26. | PoC | PoC - Implementovaný prototyp riešenia nasadený do produkčnej prevádzky a overený E2E testami minimálne s využitím mockov |
| 27. | PR | Projektové riadenie |
| 28. | ROLLOUT | ROLLOUT - Postupné pripájanie ostatných aktérov na produkčnom prostredí. |
| 29. | RFO | Register fyzických osôb |
| 30. | RPO | Register právnických osôb |
| 31. | SDL | Security development lifecycle |
| 32. | SFTP | SSH File Transfer Protocol |
| 33. | SLA | Service level agreement |
| 34. | SOAP | Simple Object Access Protocol |
| 35. | SOAR | Security orchestration, automation and response |
| 36. | SR | Slovenská republika |
| 37. | ÚV SR | Úrad vlády Slovenskej republiky |
| 38. | ŠÚ SR | Štatistický úrad Slovenskej republiky |
| 39. | VÚC | Vyšší územný celok alebo iný povoľovací orgán |

# Popis navrhovaného riešenia

Predmetom projektu je zvýšenie úrovne kybernetickej a informačnej bezpečnosti na Úrade vlády Slovenskej republiky (ďalej len „ÚV SR“). Kybernetická bezpečnosť je z pohľadu architektúry prierezovou oblasťou a teda realizuje sa skrz všetky vrstvy architektúry.

S ohľadom na vyššie uvedené bude teda predmetom projektu riešenie problematiky z nasledovných oprávnených oblastí podľa výzvy:

* Sieťová a komunikačná bezpečnosť
* Zaznamenávanie udalostí a monitorovanie

Budúce riešenie zabezpečenia informačnej a kybernetickej bezpečnosti sa bude skladať najmä z nasledovných funkcií a realizovaných činností:

**Sieťová a komunikačná bezpečnosť**

• Implementácie DDoS nástroja ako technické opatrenie za účelom zvýšenia sieťovej a komunikačnej bezpečnosti

• Implementácie Web aplikačného firewallu za účelom zvýšenia sieťovej a komunikačnej bezpečnosti

**Zaznamenávanie udalostí a monitorovanie**

• Implementácia SOCu ako nástroja na zaznamenávanie udalostí a monitorovanie

# Architektúra riešenia projektu

Architektúra riešenia projektu je spracovaná v súlade s hlavnými cieľmi motivačnej architektúry. Architektúra riešenia projektu je ďalej rozpracovaná na úrovni biznis vrstvy, aplikačnej vrstvy, technologickej vrstvy a bezpečnostnej vrstvy. Predmetom projektu je zvýšenie spôsobilosti poskytovateľa základnej služby v oblasti kybernetickej bezpečnosti a svojim rozsahom priamo reflektuje reálne potreby Úradu vlády na pasívne a aktívne posilnenie IKT. Navrhovaným riešením sú softvérové a hardvérové doplnenia IKT infraštruktúry, postupy na úpravu procesov a zníženie rizika zlyhania ľudského faktora, plošne rozvíjajúce KB kompetencie žiadateľa. Vzhľadom na charakter adresovanej problematiky je možné poskytnúť obmedzený detail rizík súčasného stavu a rovnako obmedzený detail synergických efektov a procesného nastavenia budúceho stavu.

## Biznis vrstva

**Biznis vrstva – súčasný stav:**

Úrad vlády Slovenskej republiky (ďalej „úrad vlády“) plní v zmysle kompetenčného zákona úlohy spojené s odborným, organizačným a technickým zabezpečovaním činnosti vlády Slovenskej republiky (ďalej „vláda“). Rovnaké úlohy plní úrad vlády aj pre predsedu vlády ako jeho výkonný orgán. Úrad vlády je tiež sídlom dvoch splnomocnencov vlády Slovenskej republiky: splnomocnenca vlády SR pre národnostné menšiny a splnomocnenca vlády SR pre mládež a šport. Okrem iného zabezpečuje tiež činnosť Kancelárie Bezpečnostnej rady Slovenskej republiky a činnosť sekretariátu poradných orgánov vlády, ktoré pôsobia pri úrade vlády.

Úrad vlády Slovenskej republiky je ústredným orgánom štátnej správy pre štátnozamestnanecké vzťahy a právne vzťahy pri výkone práce vo verejnom záujme, kontrolu plnenia úloh súvisiacich s výkonom štátnej správy a pre kontrolu vybavovania petícií a sťažností, koordináciu v oblasti prevencie korupcie a koordináciu uskutočňovania inklúzie marginalizovaných rómskych komunít. Kontroluje plnenie úloh z programového vyhlásenia vlády a z uznesení vlády, koordinuje prípravu zásadných opatrení na zabezpečenie hospodárskej a sociálnej politiky Slovenskej republiky, zabezpečuje a koordinuje ochranu finančných záujmov Európskej únie. Úlohy v oblasti podpory inklúzie marginalizovaných rómskych komunít vykonáva samostatná organizačná zložka Úradu vlády Slovenskej republiky, ktorá plní aj úlohy národného kontaktného bodu. Ak je Úrad vlády poverený plniť úlohy sprostredkovateľského orgánu, tieto úlohy vykonáva táto organizačná zložka, ktorej vedúci zamestnanec je štatutárnym orgánom poskytovateľa príspevkov z fondov Európskej únie.

Úrad vlády Slovenskej republiky je ústredným orgánom štátnej správy aj pre koordináciu a riadenie Plánu obnovy a odolnosti Slovenskej republiky a mechanizmu na podporu obnovy a odolnosti, koordináciu a riadenie Sociálno-klimatického fondu a vnútroštátnu implementáciu Agendy 2030. Prispieva k dlhodobej stabilite investičného prostredia prostredníctvom vypracovania Národného investičného plánu pozostávajúceho z investičných projektov strategického významu, ktoré sú kľúčové pre dlhodobý hospodársky a sociálny rozvoj Slovenska, ako aj finančného plánu pokrývajúceho identifikované investičné potreby a opierajúceho sa o rôzne finančné zdroje, a pravidelnú aktualizáciu tohto dokumentu. Úrad vlády plní úlohy strategickej a metodickej koordinácie v oblasti výskumu, vývoja a inovácií, vykonáva posudzovanie strategických iniciatív Európskej únie smerujúcich k budovaniu odolnosti Slovenska, ktorých vykonávanie vyžaduje zapojenie najmenej dvoch ústredných orgánov štátnej správy, usmerňuje a koordinuje plnenie úloh z nich vyplývajúcich, riadi a koordinuje opatrenia na tvorbu a uskutočňovanie talentovej politiky, koordinuje a riadi aktivity súvisiace s obnovou Ukrajiny a jej integráciou do Európskej únie vrátane vytvárania a prepájania príslušných finančných nástrojov na európskej a národnej úrovni. Spravuje elektronickú platformu pre verejné obstarávanie a zabezpečuje centralizované činnosti vo verejnom obstarávaní.

ÚV SR je zároveň subjektom zaradeným v registri prevádzkovateľov základných služieb podľa zákona o kybernetickej bezpečnosti č. 69/2018 Z. z. v sektore Verejná správa (https://www.nbu.gov.sk/7276-sk/zoznam-zakladnych-sluzieb/). Základná prevádzkovaná služba: webové sídlo a informačné sídlo Úradu vlády SR. ÚV SR je správca a prevádzkovateľ sietí a informačných systémov verejnej správy v pôsobnosti povinnej osoby podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.

V súlade s § 29 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „ZoKB“) prebiehal na ÚV v období od 17.10.2023 do 10.11.2023 audit kybernetickej bezpečnosti. Dňa 8.12.2023 bola ÚV odovzdaná finálna verzia záverečnej správy o výsledkoch auditu. V súlade s §29 ods. 5 ÚV SR ako prevádzkovateľ základnej služby v zákonom stanovenej lehote zaslala záverečnú správu o výsledkoch auditu NBÚ spolu s opatreniami na nápravu a s lehotami na ich odstránenie. Tento projekt rieši vybrané návrhy a opatrenia na nápravu nesúladov, ktoré majú pre ÚV SR najvyššiu prioritu a zabezpečia zvýšenie úrovne kybernetickej a informačnej bezpečnosti. V rámci poskytovaných služieb poskytuje služby prostredníctvom rôznych prístupových kanálov: elektronicky, listinne, osobne ako aj telefonicky. Pre poskytované služby ÚV SR poskytuje a realizuje viaceré biznis funkcie, kde v rámci tohto projektu je primárne relevantná biznis funkcia **Bezpečnosť**.

ÚV SR ako prevádzkovateľ základnej služby zapísanej v registri prevádzkovateľov základných služieb má povinnosti, ktoré vyplývajú zo zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „ZoKB“). Medzi základné povinnosti je prijatie a dodržiavanie všeobecných bezpečnostných opatrení pre nasledovné oblasti:

* organizácie kybernetickej bezpečnosti a informačnej bezpečnosti,
* riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
* personálnej bezpečnosti,
* riadenia prístupov,
* riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,
* bezpečnosti pri prevádzke informačných systémov a sietí,
* hodnotenia zraniteľností a bezpečnostných aktualizácií,
* ochrany proti škodlivému kódu,
* sieťovej a komunikačnej bezpečnosti,
* akvizície, vývoja a údržby informačných sietí a informačných systémov,
* zaznamenávania udalostí a monitorovania,
* fyzickej bezpečnosti a bezpečnosti prostredia,
* riešenia kybernetických bezpečnostných incidentov,
* kryptografických opatrení,
* kontinuity prevádzky,
* auditu, riadenia súladu a kontrolných činností.

Tieto bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu. ÚV SR je povinná preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených zákonom vykonaním auditu kybernetickej bezpečnosti v stanovenom rozsahu.

V súlade s § 29 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „ZoKB“) prebiehal na ÚV v období od 17.10.2023 do 10.11.2023 audit kybernetickej bezpečnosti. Dňa 8.12.2023 bola ÚV odovzdaná finálna verzia záverečnej správy o výsledkoch auditu. V súlade s § 29 ods. 5 ÚV SR ako prevádzkovateľ základnej služby v zákonom stanovenej lehote zaslala záverečnú správu o výsledkoch auditu NBÚ spolu s opatreniami na nápravu a s lehotami na ich odstránenie. Konkrétne sa jedná o vybrané opatrenia, ktoré budú realizované týmto projektom:

* Bezpečnostný dohľad a riadenie incidentov, zahŕňajúce analytické práce a rozšírenie monitoringu prostredníctvom systému SIEM.
* Hodnotenie zraniteľností a bezpečnostné aktualizácie, zamerané na zavedenie nástroja na detekovanie zraniteľností programových a technických prostriedkov.
* Zvyšovanie bezpečnosti pri prevádzke informačných systémov a sietí prostredníctvom implementácia nástrojov na riadenie bezpečnosti, evidenciu a schvaľovanie zmien.
* Nasadenie nástroja na ochranu pred kybernetickými hrozbami pomocou sandboxing mechanizmu.
* Implementácia Network Access Control (NAC) pre autentifikáciu zariadení v sieti.
* **Sieťová a komunikačná bezpečnosť:** Monitorovanie sieťovej prevádzky, detekcia anomálií pomocou strojového učenia, implementácia 2FA (dvojfaktorovej autentifikácie), bezpečné tlačenie dokumentov.
* Riešenie kybernetických bezpečnostných incidentov rozšírením antivírusovej a EDR ochrany, detailná analýza koncových zariadení.
* Implementácia nástroja na manažovanie záloh a bezpečné uloženie záloh mimo primárnej lokality.
* Zvyšovanie kompetencií zamestnancov cez rozvoj bezpečnostného povedomia a pravidelné testovanie (interné phishingové kampane).

V nadväznosti na projekt bude aktualizovaná bezpečnostná dokumentácie.

V rámci kategorizácií aktív z pohľadu dôvernosti bol vyhodnotený dopad prípadného kybernetického incidentu (najhoršieho možného scenára a dopadov na ÚV SR podľa § 24 ods. 2, písm. a) až e) ZoKB v závislosti od kategórie bezpečnostného incidentu nasledovne:

* 24 ods. 2 písm. a) zákona - **Kategória III.**
* 24 ods. 2 písm. b) a c) zákona - **Kategória III.**
* 24 ods. 2 písm. d) zákona - **Kategória III.**
* 24 ods. 2 písm. e) zákona - **Kategória III.**

Obrázok, na ktorom je text, snímka obrazovky, rovnobežný, diagram

Automaticky generovaný popis

Obrázok 1:  Model biznis architektúry (vychádza zo strategickej architektúry VS) – ASIS

**Biznis vrstva – budúci stav:**

ÚV SR identifikovala najvyššiu mieru rizika a najvyššie dopady kybernetických incidentov v sieťovej a komunikačnej bezpečnosti a v rámci zaznamenávania udalostí a monitorovania. Tieto oblasti mali aj najvyššiu mieru nesúladu s legislatívnymi požiadavkami z vykonaného auditu kybernetickej bezpečnosti.

V rámci projektu ÚV SR bude realizovať nasledovné podaktivity v súlade s oprávnenými činnosťami uvedenými vo výzve-

* Personálna bezpečnosť
* Hodnotenie zraniteľností a bezpečnostné aktualizácie
* Bezpečnosť pri prevádzke informačných systémov a sietí
* Ochrana proti škodlivému kódu
* Sieťová a komunikačná bezpečnosť
* Zaznamenávanie udalostí a monitorovanie
* Riadenie prístupov zariadení v sieti
* Riešenie kybernetických bezpečnostných incidentov (Rozšírenie existujúcej AV ochrany)
* Nasadenie nástroja na zálohovanie a uloženie záloh

Obrázok, na ktorom je text, snímka obrazovky, diagram, rovnobežný

Automaticky generovaný popis

Obrázok 2: Model biznis architektúry (vychádza zo strategickej architektúry VS) – TO BE

### Prehľad koncových služieb – budúci stav:

Projektom nie sú budované žiadne nové koncové služby. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci ÚV SR. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

### Jazyková podpora a lokalizácia

Požiadavky na jazykovú lokalizáciu riešenia a používateľské prostredie služieb bude implementované v slovenskom jazyku.

## Aplikačná vrstva

Aplikačná vrstva ÚV SR pozostáva z viacerých informačných systémov podporujúcich výkon funkcií a činností definovaných na úrovni biznis architektúry. Je rozdelené primárne do nasledujúcich oblastí.

**Moduly front-endu**: predstavujú špecifické, najmä rezortné komponenty pre interakciu s používateľmi, čiže komponenty, ktoré nie sú spoločné a zdieľané viacerými inštitúciami (napr. rezortné portály).

**Externé systémy**: externé systémy integrované so systémami ÚV SR

**Spoločné moduly front-endu**: združujú spoločné komponenty, ktoré riešia interakciu s používateľmi (občanmi, podnikateľmi a zamestnancami verejnej správy)

**Integrácia a orchestrácia**: rieši integráciu a vzájomnú interoperabilitu informačných systémov verejnej správy SR na úrovni aplikačnej a dátovej integrácie a zabezpečuje služby orchestrácie najmä pre životné situácie.

**Agendové informačné systémy**: podporujú výkon konkrétnej agendy a realizujú kľúčové aplikačné služby.

**Moduly back-endu**: predstavujú špecifické, najmä rezortné komponenty pre podporu špecifických back office činností, čiže komponenty, ktoré nie sú spoločné a zdieľané viacerými organizáciami. Tu patria aj nástroje pre kybernetickú a informačnú bezpečnosť.

Obrázok, na ktorom je text, snímka obrazovky, diagram, rad

Automaticky generovaný popis

Obrázok 3: Aplikačná architektúra budúceho stavu

### Rozsah informačných systémov – AS IS

Nie je relevantné pre projekt. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

### Rozsah informačných systémov – TO BE

Nie je relevantné pre projekt. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

V rámci projektu budú implementované nové nástroje pre zvýšenie úrovne kybernetickej a informačnej bezpečnosti.

### Využívanie nadrezortných a spoločných ISVS – AS IS

Nie je relevantné pre projekt. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

### Prehľad plánovaných integrácií ISVS na nadrezortné ISVS – spoločné moduly podľa zákona č. 305/2013 e-Governmente – TO BE

Nie je relevantné pre projekt. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

### Prehľad plánovaného využívania iných ISVS (integrácie) – TO BE

Nie je relevantné pre projekt. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

### Aplikačné služby pre realizáciu koncových služieb – TO BE

Nie je relevantné pre projekt. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

### Aplikačné služby na integráciu – TO BE

Nie je relevantné pre projekt. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

### Poskytovanie údajov z ISVS do IS CSRÚ – TO BE

Projektom nie je plánované poskytovanie údajov do IS CSRÚ. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

### Konzumovanie údajov z IS CSRU – TO BE

Nie je relevantné pre projekt. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

## Dátová vrstva

Nie je relevantné pre projekt. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

### Údaje v správe organizácie

Zavedenie systematického manažmentu údajov nie je predmetom navrhovaného projektu. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

### Dátový rozsah projektu - Prehľad objektov evidencie - TO BE

Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

### Referenčné údaje

Projektom nie sú plánované žiadne nové referenčné údaje ani údaje, ktoré je možné vyhlásiť za referenčné. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

### Kvalita a čistenie údajov

Cieľom projektu nie je systematický manažment údajov z hľadiska citlivosti kvality údajov a čistenia údajov. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

### Otvorené údaje

Nie je relevantné pre projekt, nebudú poskytované žiadne nové Otvorené údaje. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

### Analytické údaje

Nie je relevantné pre projekt, nebudú poskytované žiadne nové Analytické údaje. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

### Moje údaje

Nie je relevantné pre projekt, nebudú poskytované žiadne nové Moje údaje. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

### Prehľad jednotlivých kategórií údajov

Projekt nie je zameraný na systematický manažment údajov, nemení štruktúru ani obsah údajov. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov.

## Technologická vrstva

### Prehľad technologického stavu - AS IS

Súčasťou projektu je tiež doplnenie jednotlivých HW položiek pre potreby rozšírenia vrstvy. V projekte nedochádza k zmene architektúry technologickej vrstvy. Z dôvodu, že s jedná o projekt kybernetickej bezpečnosti detailný popis jednotlivých HW položiek na vyžiadanie.

### Požiadavky na výkonnostné parametre, kapacitné požiadavky – TO BE

V rámci navrhovaného riešenia sa predpokladá zachovanie súčasných výkonnostných požiadaviek a kapacitných požiadaviek.

### Návrh riešenia technologickej architektúry

Technologická architektúra sa oproti súčasnému stavu nemení a bude prevádzkovaná v rovnakom technologickom prostredí. Technologická vrstva budúceho stavu vychádza zo súčasného stavu a bude podporená novými nasadenými nástrojmi prevádzkovanými na viacerých technológiách.

Obrázok, na ktorom je text, snímka obrazovky, diagram, písmo

Automaticky generovaný popis

Obrázok 5: Návrh riešenia technologickej architektúry ÚV SR

### Využívanie služieb z katalógu služieb vládneho cloudu

Projekt nebude využívať služby z katalógu vládneho cloudu. Cieľom projektu sa realizuje zvýšenie kybernetickej a informačnej bezpečnosti v rámci celej organizácie. Nedochádza k rozširovaniu koncových alebo aplikačných služieb, funkcionalít v rámci agendových systémov, ani k zmene evidovaných a poskytovaných údajov. Implementované nástroje budú prevádzkované v infraštruktúre ÚV SR bez potreby jej rozšírenia.

## Bezpečnostná architektúra

Vzhľadom na verejný charakter projektovej dokumentácie nie je možné poskytnúť detailnú špecifikáciu súčasného technologického stavu a mieru zraniteľnosti z pohľadu kybernetickej a informačnej bezpečnosti. Navrhované opatrenia v budúcom stave majú za cieľ zabezpečiť súlad aplikačnej a technologickej infraštruktúry s požiadavkami zákona o kybernetickej bezpečnosti, súvisiacich legislatívnych noriem a výsledkov samohodnotenia v zmysle zákona o kybernetickej bezpečnosti.

Za účelom zvýšenia úrovne zavedených postupov a opatrení týkajúcich sa kybernetickej a informačnej bezpečnosti je potrebné konsolidovať existujúcu bezpečnostnú architektúru a dobudovať ekosystému riadenia informačnej bezpečnosti implementáciou nových a inováciou existujúcich bezpečnostných nástrojov a procesov, a to najmä v nasledovných oblastiach a v súlade s nálezmi sebahodnotenia. Riešenie zabezpečenia prevádzkovaných ISVS v správe ÚV SR je rozdelené do viacerých častí, pričom každá časť komplexne pokrýva danú oblasť. Jedná sa o nasledovné hlavné oblasti:

**Popis jednotlivých blokov implementovanej bezpečnostnej architektúry, realizovaných oprávnených aktivít a požiadaviek na jednotlivé technológie:**

Projekt teda poskytne komplexnú ochranu na viacerých úrovniach a výrazne zvýši schopnosti verejného obstarávateľa odolávať moderným kybernetickým hrozbám, chrániť citlivé údaje a efektívne riadiť prístupy a oprávnenia v rámci celej organizácie. Služby a funkcie uvedené v tejto kapitole poskytujú z dôvodu, že sa jedná o projekt kybernetickej bezpečnosti len základné informácie a základný architektonický rámec riešenia, ktoré by malo byť implementované projektom. Budúce riešenie zabezpečenia informačnej a kybernetickej bezpečnosti sa bude skladať najmä z nasledovných funkcií a realizovaných činností:

**Personálna bezpečnosť**

* Zvyšovanie kompetencií zamestnancov prostredníctvom rozvoja bezpečnostného povedomia a pravidelného testovanie použitím interných phisingových kampaní.

**Hodnotenie zraniteľností a bezpečnostné aktualizácie**

* Zavedenie nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí a detegovanie existujúcich zraniteľností technických prostriedkov a ich častí (cca. 512 IP).

**Bezpečnosť pri prevádzke informačných systémov a sietí**

* Implementácia technických riešení podporujúcich riadenie bezpečnosti pri prevádzke, napr. nástroj pre riadenie, evidenciu a schvaľovanie zmien. (850 používateľov)

**Ochrana proti škodlivému kódu**

* Implementácia nástroja na ochranu pred kybernetickými hrozbami prostredníctvom mechanizmu „sandboxing“, 2 zariadenie, kde každé musí spracovať aspoň 1300 unikátnych súborov za hodinu.

**Sieťová a komunikačná bezpečnosť**

* Implementácia nástroja na monitorovanie sieťovej prevádzky prostredníctvom dedikovaných sondovacích zariadení s cieľom identifikovať anomálie a potencionálne škodlivú činnosť na základe výstupov algoritmov strojového učenia (NDR), pričom by malo byť schopné aspoň spracovať 100000 flows za sekundu.
* Implementácia riešenia na monitorovanie sieťovej prevádzky prostredníctvom dedikovaných sondovacích zariadení s cieľom identifikovať škodlivú činnosť na základe známych vzoriek škodlivej sieťovej prevádzky (IPS) s priepustnosťou 1GB.
* Implementácia nástroja SW/HW riešenia 2FA (napr. formou mobilnej aplikácie) na kontrolu vzdialeného prístupu na strane používateľov pri prístupe k IS. (cca. 850 používateľov).

**Zaznamenávanie udalostí a monitorovanie**

* Implementácia centrálneho nástroja na zaznamenávanie činností sietí a informačných systémov a používateľov a identifikovanie bezpečnostných incidentov (SIEM) ako aj zber a ukladanie logov z jednotlivých informačných systémov; on premise, zber minimálne zo 100 zariadení. SIEM bude monitorovať a korelovať všetky typy logovaných udalostí, vrátane rôznych OS (Windows, Unix) a zariadení (IDS/IPS, FW a pod.).
* Implementácia automatizovaných systémov vykonávajúcich dohľad pred neoprávnenými zásahmi, neautorizovaným prístupom, najmä pred zmenami a zničením, vrátane monitorovania kapacity systémov a návrh adekvátnych opatrení na ukladanie záznamov a systému logovania (70 zariadení).

**Riadenie prístupov zariadení v sieti**

* Implementácia Network Acces Control (NAC) v súlade so štandardom IEEE 802.1x pre cca 850 zariadení, vrátane technologického vybavenia pre autentifikáciu zariadení v sietí.

**Riešenie kybernetických bezpečnostných incidentov (Rozšírenie existujúcej AV ochrany)**

* Rozšírenie licencií existujúceho AV/EDR riešenia na koncových staniciach (cca 850 zariadení) a serveroch (cca 70 serverov)
* Threat inteligence, Zerotrust ochranu (komplexné riadenie prístupu na internet) a zbieranie digitálnych dôkazov z koncových bodov (forenzná analýza). Súčasťou riešenia bude aj detailné preverenie, analýza a diagnostika všetkých koncových zariadení z pohľadu prípadnej aktuálnej infekcie malvérom a jeho odstránenia. (cca. 850 zariadení).

**Nasadenie nástroja na zálohovanie a uloženie záloh**

* Nasadenie nástroja pre manažovanie a automatické spúšťanie záloh systémov a dát a rovnako aj technologické vybavenie pre bezpečné uloženie záloh v primárnej lokalite a zároveň aj v inej lokalite mimo primárnych systémov formou automatickej replikácie záloh do tejto vzdialenej, celková použiteľná kapacita min 70TB,

Náhľad technologickej to be vrstvy architektúry:

Obrázok, na ktorom je text, snímka obrazovky, diagram, nalepovacie lístočky

Automaticky generovaný popis

Bezpečnostná architektúra budúceho stavu bude v súlade s dotknutými právnymi normami a zároveň s technickými normami, ktoré stanovujú úroveň potrebnej bezpečnosti IS, pre manipuláciu so samotnými dátami, alebo technické / technologické / personálne zabezpečenie samotnej výpočtovej techniky/HW vybavenia. Ide najmä o:

* zákon č. 95/2019 Z.z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
* zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
* zákon č. 45/2011 Z.z. o kritickej infraštruktúre
* vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy
* vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy
* vyhláška Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov
* nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
* zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.
* smernica Európskeho parlamentu a Rady (EÚ) (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2)
* zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej aj „zákon o kybernetickej bezpečnosti“),
* vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby),
* vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov,
* vyhláška Národného bezpečnostného úradu č. 264/2023 Z. z. ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
* vyhláška Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti,
* zákon č. 301/2023 Z. z. ktorým sa mení a dopĺňa zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony,
* vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy,
* vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
* nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) – GDPR,
* zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
* Metodika analýzy rizík kybernetickej bezpečnosti - Metodika analýzy rizík pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti (NBÚ)

Projektom sa zvyšuje úroveň kybernetickej a informačnej bezpečnosti nasadením resp. rozšírením nástrojov pre pokrytie kompletnej organizácie ÚV SR a pre oblasti: sieťovej a komunikačnej bezpečnosti a zaznamenávaní udalostí a monitorovaní. V nadväznosti na projekt bude aktualizovaná bezpečnostná dokumentácia pre jednotlivé oblasti, ktorá vyplýva zo systému riadenia informačnej (a kybernetickej) bezpečnosti v súlade s vyhlášku Národného bezpečnostného úradu č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

# Závislosti na ostatné ISVS / projekty

Predkladaný projekt nie je závislý na iných pripravovaných resp. prebiehajúcich projektoch.

# Zdrojové kódy

Projektom bude zvýšená úroveň kybernetickej a informačnej bezpečnosti, ktorý pozostáva z nákupu krabicových balíkov, ktoré budú dodávateľom nasadené do prevádzky. Vzhľadom na to, že predmetom nie je vývoj na mieru informačného systému je táto kapitola irelevantná.

# Prevádzka a údržba

Prevádzka a údržba navrhnutého riešenia projektu bude zabezpečená internými personálnymi kapacitami na úrovni podpory L1 až L3 (L3 externe). Pre hlásenie problémov bude využívaný Helpdesk. Predpoklad riešenia problémov a požiadaviek bude od nahlásenia problému alebo požiadavky prostredníctvom helpdesku (e-mailom, telefonicky, formulárom), identifikácia a preverenie problému/požiadavky, vykonanie opravy/podpory.

ÚV SR v súčasnosti disponuje interným zamestnancom: Manažér kybernetickej a informačnej bezpečnosti.

## Prevádzkové požiadavky

Prevádzkové požiadavky budú zabezpečené na úrovni podpory L1, L2 a L3.

### Úrovne podpory používateľov

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

* **L1 podpora** - začiatočná úroveň podpory, ktorá je zodpovedná za riešenie základných problémov a požiadaviek koncových užívateľov a ďalšie služby vyžadujúce základnú úroveň technickej podpory. Základnou funkciou podpory 1. stupňa je zhromaždiť informácie, previesť základnú analýzu a určiť príčinu problému a jeho klasifikáciu. Typicky sú v úrovni L1 riešené priamočiare a jednoduché problémy a základné diagnostiky, overenie dostupnosti jednotlivých vrstiev infraštruktúry (sieťové, operačné, vizualizačné, aplikačné atď.) a základné užívateľské problémy (typicky zabudnutie hesla), overovanie nastavení SW a HW atď.
* **L2 podpora** - riešiteľské tímy s hlbšou technologickou znalosťou danej oblasti. Riešitelia na úrovni Podpory L2 nekomunikujú priamo s koncovým užívateľom, ale sú zodpovední za poskytovanie súčinnosti riešiteľom 1. úrovne podpory pri riešení eskalovaného hlásenia, čo mimo iného obsahuje aj spätnú kontrolu a podrobnejšiu analýzu zistených dát predaných riešiteľom 1. úrovne podpory. Výstupom takejto kontroly môže byť potvrdenie, upresnenie, alebo prehodnotenie hlásenia v závislosti na potrebách Objednávateľa. Primárnym cieľom riešiteľov na úrovni Podpory L2 je dostať Hlásenie čo najskôr pod kontrolu a následne ho vyriešiť - s možnosťou eskalácie na vyššiu úroveň podpory – Podpora L3.
* **L3 podpora** - Podpora 3. stupňa predstavuje najvyššiu úroveň podpory pre riešenie tých najobťažnejších hlásení, vrátane prevádzania hĺbkových analýz a riešenie extrémnych prípadov, ktorú bude zabezpečovať výrobca implementovaných nástrojov.

Prevádzka implementovaných nástrojov v rámci projektu L1 až L3 bude zabezpečená internými zamestnancami ÚV SR. V prípade nevyhnutnej potreby bude zabezpečená L3 podpora výrobcu implementovaných nástrojov, ktorá bude financovaná z vlastných zdrojov ÚV SR.

### Riešenie incidentov – SLA parametre

Za incident je považovaná chyba IS, t.j. správanie sa v rozpore s prevádzkovou a používateľskou dokumentáciou IS. Za incident nie je považovaná chyba, ktorá nastala mimo prostredia IS napr. výpadok poskytovania konkrétnej služby Vládneho cloudu alebo komunikačnej infraštruktúry.

Označenie naliehavosti incidentu:

|  |  |  |
| --- | --- | --- |
| **Označenie naliehavosti incidentu** | **Závažnosť incidentu** | **Popis naliehavosti incidentu** |
| **A** | **Kritická** | Je to vada spôsobená vážnou chybou a/alebo nedostatkom dodávanej softvérovej aplikácie, pričom táto chyba a/alebo nedostatok zabraňuje používaniu dodávanej softvérovej aplikácie. Nie je možné poskytnúť požadovaný výstup z IS. |
| **B** | **Vysoká** | Je vada, spôsobená chybou a/alebo nedostatkom dodávanej softvérovej aplikácie, pričom táto chyba a/alebo nedostatok obmedzuje používanie dodávanej softvérovej aplikácie nasledovne:  Niektoré aplikačné funkcie (moduly, komponenty, objekty, programy) dodávanej softvérovej aplikácie nie sú funkčné alebo nie je umožnený prístup k niektorej aplikačnej funkcii (modulu, komponentu, objektu, programu) dodávanej softvérovej aplikácie  alebo  (ii) Nie je možné vykonať výber niektorých údajov alebo nie je možné vyhotoviť niektorý výstup z databázy údajov dodávanej softvérovej aplikácie alebo nie je možné vykonať prístup k niektorým údajom v databáze údajov dodávanej softvérovej aplikácie.  napr. tlač pomocných výstupov, zostavy, funkčnosť nesúvisiaca s vyrubením a pod. |
| **C** | **Stredná** | Do tejto kategórie spadajú všetky chyby a/alebo nedostatky spojené s používaním dodávanej softvérovej aplikácie, ktoré nie sú klasifikované ako závažné alebo kritické vady, pričom však čiastočne obmedzujú používanie dodávanej softvérovej aplikácie a vyžadujú si:  Nastavenie parametrov systému Poskytovateľom alebo  (ii) Vzniknutá vada a/alebo nedostatok má za príčinu miernu nepohodlnosť pri práci so softvérovou aplikáciou, ktorá je však funkčná. |

možný dopad:

|  |  |  |
| --- | --- | --- |
| **Označenie závažnosti incidentu** | **Dopad** | **Popis dopadu** |
| **1** | **katastrofický** | katastrofický dopad, priamy finančný dopad alebo strata dát, |
| **2** | **značný** | značný dopad alebo strata dát |
| **3** | **malý** | malý dopad alebo strata dát |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Matica priority incidentov** | | **Dopad** | | |
| **Katastrofický - 1** | **Značný - 2** | **Malý - 3** |
| **Naliehavosť** | **Kritická - A** | 1 | 2 | 3 |
| **Vysoká - B** | 2 | 3 | 3 |
| **Stredná - C** | 2 | 3 | 4 |

**Vyžadované reakčné doby:**

|  |  |  |  |
| --- | --- | --- | --- |
| **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 verejným obstarávateľom (vrátane užívateľov IS, ktorí nie sú v pracovnoprávnom vzťahu s verejným obstarávateľom) na helpdesk úrovne L3 a jeho prevzatím na riešenie.
* (2) DKVI znamená obnovenie štandardnej prevádzky - čas medzi nahlásením incidentu verejným obstarávateľom a vyriešením incidentu úspešným uchádzačom (do doby, kedy je funkčnosť prostredia znovu obnovená v plnom rozsahu). Doba konečného vyriešenia incidentu od nahlásenia incidentu verejným obstarávateľom (DKVI) sa počíta počas celého dňa. Do tejto doby sa nezarátava čas potrebný na nevyhnutnú súčinnosť verejného obstarávateľa, ak je potrebná pre vyriešenie incidentu. V prípade potreby je úspešný uchádzač oprávnený požadovať od verejného obstarávateľa 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 verejným obstarávateľom úspešnému uchádzačovi v rámci testovacieho prostredia

1. Majú prioritu 3 a nižšiu
2. Vzťahujú sa výhradne k dostupnosti testovacieho prostredia
3. Za incident na testovacom prostredí sa nepovažuje incident vztiahnutý k práve testovanej funkcionalite.

Vyššie uvedené SLA parametre nebudú použité pre nasledovné služby:

* Služby systémovej podpory na požiadanie (nad paušál)
* Služby realizácie aplikačných zmien vyplývajúcich z legislatívnych a metodických zmien (nad paušál)

Pre tieto služby budú dohodnuté osobitné parametre dodávky.

## Požadovaná dostupnosť IS:

|  |  |  |
| --- | --- | --- |
| **Popis** | **Parameter** | **Poznámka** |
| **Prevádzkové hodiny** | 8 hodín | Po – Pia, 8:00 - 16:00 |
| **Servisné okno** | 14 hodín | od 17:00 hod. - do 7:00 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** | 97% | * 97% z 24/7/365 t.j. max ročný výpadok je 10,95 dňa. Maximálny mesačný výpadok je 21,9 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. |

### Dostupnosť (Availability)

Dostupnosť znamená, že dáta sú prístupné v okamihu jej 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 97% dostupnosť znamená výpadok 10,95 dňa.

### RTO (Recovery Time Objective)

V rámci projektu sa očakáva tradičné zálohovanie - výpadok a obnova trvá cca hodiny až dni.

### RPO (Recovery Point Objective)

V rámci projektu sa očakáva tradičné zálohovanie - výpadok a obnova trvá cca hodiny až dni.

# Požiadavky na personál

**Riadiaci výbor** projektu tvorí predseda riadiaceho výboru projektu a vlastníci procesov alebo nimi poverení zástupcovia.

Riadiaci výbor sa riadi “Štatútom riadiaceho výboru”, ktorý je popísaný v dokumente Štatút RV projektu ako najvyšší riadiaci orgán na účely realizácie projektu na základe schválenej projektovej dokumentácie.

Štatút Riadiaceho výboru upravuje najmä jeho pôsobnosť, úlohy, zloženie, zasadnutie a hlasovanie. Členom riadiaceho výboru projektu môže byť aj zástupca dodávateľa. Väčšina členov riadiaceho výboru projektu s hlasovacím právom sú osoby navrhnuté objednávateľom a zastupujú záujmy objednávateľa. Riadiaci výbor projektu dozerá na hospodárnosť, efektívnosť a účelové využívanie finančných prostriedkov a môže prispôsobiť štandardy projektového riadenia na realizovaný projekt.

Riadiaci výbor má minimálne 5 členov, vrátane predsedu Riadiaceho výboru (ďalej len „predseda“) :

Riadiaci výbor projektu môžu tvoriť:

* 1. **predseda** Riadiaceho výboru projektu,
  2. **podpredseda** Riadiaceho výboru projektu,
  3. **vlastník alebo vlastníci procesov ÚV** (biznis vlastník infraštruktúra) alebo nimi poverený zástupca alebo zástupcovia,
  4. **zástupcu kľúčových používateľov** (end user),
  5. zástupca za Dodávateľa v zmysle Zmluvy o Dielo s Dodávateľom.
  6. projektový manažér prijímateľa.

Riadiaci výbor je riadený predsedom, ktorým je zástupca Objednávateľa. 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. Na rokovanie Riadiaceho výboru môžu byť v prípade potreby prizvaní aj iní účastníci tak zo strany Objednávateľa alebo za stranu Dodávateľa.

Riadiaci výbor zasadá pravidelne, spravidla raz za mesiac avšak najmenej jedenkrát za tri (3) po sebe nasledujúce kalendárne mesiace. Zasadnutie Riadiaceho výboru zvoláva predseda. 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.

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.

Program zasadnutia a pracovné materiály Riadiaceho výboru distribuuje Asistent projektového manažéra na základe podkladov a inštrukcií predsedu alebo toho člena Riadiaceho výboru, ktorý požiadal o zasadnutie Riadiaceho výboru.

Asistent projektového manažéra zabezpečí ich distribúciu členom Riadiaceho výboru najneskôr 3 pracovné dni pred zasadnutím Riadiaceho výboru. Za vecnú správnosť distribuovaného materiálu zodpovedá člen Riadiaceho výboru, ktorý ho predkladá.

Riadiaci výbor zaniká ukončením plnohodnotnej implementácie projektu a jeho uvedením do produktívnej prevádzky. Zoznam členov Riadiaceho výboru je súčasťou dokumentu Komunikačná matica uloženom na zdieľanom projektovom úložisku.

| **ID** | **MENO A PRIEZVISKO** | **POZÍCIA** | **ORGANIZAČNÝ ÚTVAR** | **ROLA V PROJEKTE S UVEDENÍM HLASOVACIEHO PRÁVA** |
| --- | --- | --- | --- | --- |
| 1. | TBD | TBD | TBD | Predseda RV (HP) |
| 2. | TBD | TBD | TBD | Podpredseda RV (HP) |
| 3. | TBD | TBD | TBD | Zástupca vlastníkov procesov (HP) |
| 4. | TBD | TBD | TBD | Zástupca vlastníkov procesov II. (HP) |
| 5. | TBD | TBD | TBD | Zástupcu kľúčových používateľov |
| 6. | TBD | TBD | TBD | Zástupca Dodávateľa |
| 7. | TBD | Projektový manažér | TBD | Projektový manažér prijímateľa |

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 vývojom dodávaného Diela, vrátane kvality), finančného riadenia a monitorovania realizácie projektu v zmysle riadenia podľa vyhlášky MIRRI č. 401/2023 Z. z. v platnom znení.

Projektový tím bude pozostávať z pozícií:

* Projektové role:
* Projektový manažér,
* Kľúčový používateľ,
* Manažér kybernetickej a informačnej bezpečnosti,
* Ďalšie projektové role:
* Finančný manažér
* Asistent PM

V súlade s výzvou ÚV SR zabezpečí, aby počas implementácie projektu a po jeho skončení (počas obdobia udržateľnosti) bol k dispozícii interný personál na obsluhu, prevádzku a rozvoj riešenia. Zároveň bude minimálne počas obdobia udržateľnosti zabezpečené financovanie tohto personálu zo zdrojov ÚV SR.

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 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** | **PROJEKTOVÁ ROLA** |
| 1. | TBD | Projektový manažér | Odbor informačných technológií | Projektový manažér |
| 2. | TBD | Špecialista v oblasti počítačových sietí | Odbor informačných technológií | Kľúčový používateľ |
| 3. | TBD | Manažér kybernetickej a informačnej bezpečnosti | Odbor informačných technológií | Manažér kybernetickej a informačnej bezpečnosti |
| 4. | TBD | TBD | TBD | Finančný manažér |
| 5. | TBD | TBD | TBD | Asistent PM |

RV je riadiaci orgán projektu, ktorý zodpovedá najmä za splnenie stanovených cieľov projektu, rozhoduje o zmenách, ktoré majú zásadný význam a prejavujú sa hlavne dopadom na časový harmonogram a finančné prostriedky projektu. Reprezentuje najvyššiu akceptačnú autoritu projektu. Štatút Riadiaceho výboru projektu upravuje najmä úlohy, zloženie a pôsobnosť RV, ako aj práva a povinnosti členov RV pri riadení a realizácii predmetného projektu.

Projektový manažér riadi projekt, kvalitu a riziká projektu a zabezpečuje plnenie úloh uložených RV. Členovia projektového tímu zabezpečujú plnenie úloh uložených projektovým manažérom, alebo RV.

Ďalšie povinnosti členov RV, projektového manažéra a členov projektového tímu sú uvedené vo Vyhláške č. 401/2023 Z. z. a v doplňujúcich vzoroch a šablónach zverejnených na webovom sídle MIRRI SR.

|  |  |
| --- | --- |
| **Projektová rola:** | **PROJEKTOVÝ MANAŽÉR** |
| Detailný popis rozsahu zodpovedností, povinností a kompetencií: | - zodpovedá za každodenné riadenie projektu v mene RV, za monitorovanie projektu, za plánovanie aktivít, za informovanie o projekte, atď.,  - zodpovedá za určenie pravidiel, spôsobov, metód a nástrojov riadenia projektu a získanie podpory RV pre riadenie, plánovanie a kontrolu projektu a efektívne využívanie projektových zdrojov (ľudských a finančných),  - zodpovedá za splnenie všetkých legislatívnych požiadaviek (právne predpisy SR), metodických požiadaviek súvisiacich s implementáciou projektu a formálnu administráciu projektu súvisiacu s riadením, organizovaním, finančným zúčtovaním, sledovaním čiastkových a celkových výsledkov (monitorovaním) a hodnotením výsledkov,  - integrovane riadi prípravu a uskutočnenie projektu, nasadenie disponibilných prostriedkov, zabezpečuje koordináciu dodávateľov a zhotoviteľov jednotlivých výstupov projektu, zabezpečuje koordináciu partnerov, časový priebeh a kvalitu výstupov projektu, zmeny projektu a rieši konflikty s okolím projektu,  - prijíma rozhodnutia a riadi projekt tak, aby sa splnili stanovené ciele projektu, a aby projekt dodával dohodnuté produkty v dohodnutej kvalite, v čase, a v rámci rozpočtu,  - zodpovedá RV za plnenie cieľov projektu a celkový postup prác v projekte,  - informuje RV o stave a priebehu projektu, predkladá návrhy na zlepšenie,  - riadi strategické a projektové riziká, vrátane vývojových a rezervných plánov,  - zodpovedá za identifikovanie kritických miest projektu a navrhovanie ciest k ich eliminácii,  - aktívne komunikuje s dodávateľom, zástupcom dodávateľa a projektovým manažérom dodávateľa s cieľom zabezpečiť úspešné dodanie a nasadenie požadovaných projektových výstupov,  - zabezpečuje kontrolu dodržiavania a plnenia míľnikov v zmysle zmluvy s dodávateľom,  - zabezpečuje vecnú administráciu zúčtovania dodávateľských faktúr,  - predkladá požiadavky dodávateľa na rokovanie RV,  - zodpovedá za koordináciu a zabezpečenie podkladov pre oddelenie komunikačné pre potreby medializácie projektu,  - zodpovedá za informovanie zamestnancov a verejnosti o začatí a ukončení projektu v závislosti od jeho charakteru,  - zodpovedá za zabezpečenie vypracovania, priebežnej aktualizácie a verzionovania manažérskej a špecializovanej dokumentácie a produktov,  - pripravuje a predkladá stanovené dokumenty na schválenie RV,  - navrhuje zaradiť projekt alebo jeho časť do režimu utajenia,  - zabezpečuje permanentný dohľad a zvýšenú mieru kontroly a ochrany tokov informácií pri realizácii utajovaného projektu alebo utajovanej časti projektu,  - zodpovedá za vypracovanie požiadaviek na zmenu, návrh ich prioritizácie a predkladanie zmenových požiadaviek na rokovanie RV,  - zabezpečuje podanie žiadosti o rozpočtové opatrenie MF SR cez Rozpočtový informačný systém na projekt IT podľa potreby,  - zodpovedá za riadenie zmeny a prípadné požadované riadenie konfigurácií,  - navrhuje členov projektového tímu po dohode s líniovým vedúcim a tímovým manažérom a tiež navrhuje rozsah ich zodpovedností a činností,  - organizuje, riadi, motivuje projektový tím a deleguje úlohy členom projektového tímu,  - hodnotí členov projektového tímu,  - udeľuje pokyny na výkon činností projektovej kancelárie,  - podľa potreby deleguje svoje povinnosti a práva na tímových manažérov a koordinuje ich činnosť,  - plní úlohy tímového manažéra (vedúceho projektového tímu), ak takáto rola v projekte nie je obsadená –viď činnosť projektovej role „Tímový manažér“,  - monitoruje výkonnosť projektu, to znamená, že sleduje pokrok vo vybraných ukazovateľoch (KPI) projektu a predkladá ho na schválenie RV,  - zabezpečuje evidenciu v informačných systémoch pre štandardizované procesy programové a projektového riadenia, napr. IT monitorovací systém pre európske štrukturálne a investičné fondy,  - zodpovedá za publikovanie RV schválených projektových výstupov v MetaIS chronologicky, z každej fázy životného cyklu projektu,  - zodpovedá za publikovanie zápisov RV v MetaIS,  - počas celej doby realizácie projektu štandardne zabezpečuje nasledovné prierezové činnosti:  1. kontinuálne zdôvodňovanie projektu, ktoré zahŕňa posúdenie, či je projekt požadovaný a dosiahnuteľný, potrebné na rozhodovanie o pokračovaní vynakladania prostriedkov počas všetkých fáz projektu, vypracované aspoň po ukončení každej fázy projektu,  2. plánovanie a operatívne riadenie dodávania projektových produktov,  3. riadenie rizík a závislostí, ktoré zahŕňa identifikáciu, hodnotenie a riadenie rizík, závislostí a hrozieb na úspešnú realizáciu projektu,  - zabezpečuje dodržiavanie legislatívno-metodických zásad pre riadenie projektov,  - zodpovedá za formálnu administráciu projektu, riadenie centrálneho úložiska projektovej dokumentácie ÚV SR, správu a archiváciu projektovej dokumentácie,  - sleduje dodržiavanie interných riadiacich aktov. |

|  |  |
| --- | --- |
| **Projektová rola:** | **KĹÚČOVÝ POUŽÍVATEĽ** |
| Stručný popis: | * reprezentuje záujmy budúcich koncových používateľov projektových produktov alebo projektových výstupov, * poskytuje súčinnosť pri spracovaní interného riadiaceho aktu upravujúceho prevádzku, servis a podporu IT, * aktívne sa zúčastňuje stretnutí projektového tímu a spolupracuje na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Prílohou č.1 tejto smernice, * plní pokyny PM a dohody zo stretnutí projektového tímu. |
| Detailný popis rozsahu zodpovedností, povinností a kompetencií | * návrh a špecifikáciu funkčných, nefunkčných a technických požiadaviek, potreby, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu, požiadaviek koncových používateľov na prínos systému a požiadaviek na bezpečnosť, * jednoznačnú špecifikáciu požiadaviek na jednotlivé projektové výstupy (špecializované produkty a výstupy) z pohľadu vecno-procesného a legislatívy, * návrh a definovanie rizík, rozhraní a závislostí, * vykonanie používateľského testovania funkčného používateľského rozhrania (UX testovania) a za finálne odsúhlasenie používateľského rozhrania, * návrh a definovanie akceptačných kritérií, * akceptačné testovanie (UAT) a návrh na akceptáciu projektových produktov alebo projektových výstupov a finálny návrh na spustenie do produkčnej prevádzky, * 7. predkladanie požiadaviek na zmenu funkcionalít produktov, |

|  |  |
| --- | --- |
| **Projektová rola:** | **PROJEKTOVÁ KANCELÁRIA („PMO“)** |
| Projektovou kanceláriou je príslušný organizačný útvar FR SR v zmysle organizačného poriadku FR SR, ktorý zabezpečuje podporu riadenia projektu, najmä: | - administratívnu a technickú podporu v jednotlivých fázach životného cyklu projektu,  - vypracovanie a odovzdanie menovacích dekrétov a odvolacích dekrétov  pre predsedu RV, členov RV, PM a podpísaných predsedom RV pre členov projektového tímu a PMO,  - zabezpečenie oboznámenia predsedu RV, členov RV, a členov projektového tímu s projektom, ich  úlohami a rozsahom ich zodpovedností, atď. podľa pokynu PM,  - organizačné zabezpečenie zasadnutí RV, spracovanie zápisov zo zasadnutí RV a zabezpečenie ich  zverejnenia prostredníctvom MetaIS, ak je to potrebné,  - organizačné zabezpečenie stretnutí realizovaných v rámci projektu, spracovanie zápisov z týchto  stretnutí,  - vykonávanie úloh na základe pokynov PM,  - vypracovanie a aktualizácia zoznamov úloh, rizík, otvorených otázok a iných manažérskych správ,  reportov, zoznamov a požiadaviek,  - organizačné zabezpečenie pripomienkového konania projektovej dokumentácie,  - správu projektov, monitorovanie stavu projektu, udržiavanie aktuálnosti a hodnovernosti údajov  o projektoch a podľa potreby optimalizáciu projektov,  - prípravu informácií o stave realizácie projektu podľa potreby,  - zhromaždenie, analyzovanie a vyhodnotenie poznatkov z implementácie projektov a definovanie  ponaučenia za účelom predchádzania a opakovania chýb z minulosti,  - zabezpečenie zverejnenia projektových výstupov jednotlivých fáz životného cyklu projektu na centrálnom  úložisku projektovej dokumentácie ÚV SR a v MetaIS, ak je to potrebné,  - poskytuje súčinnosť PM pri predkladaní projektových produktov na posúdenie ekonomickej výhodnosti  a súladu s programovým riadením MIRRI SR, ak je to potrebné,  - organizáciu procesov súvisiacich s výkazmi práce členov projektových tímov jednotlivých projektov,  - vytvorenie a spravovanie centrálneho úložiska projektovej dokumentácie ÚV SR,  - vytvorenie komunikačnej platformy v rámci projektu a medzi projektami navzájom,  - zabezpečenie interakcie medzi zainteresovanými stranami, ich spokojnosť a realizáciu požiadaviek  spojených s implementáciou projektu,  - spoluprácu s metodickou podporou projektového riadenia,  - zabezpečenie uloženia originálov projektovej dokumentácie. |

|  |  |
| --- | --- |
| **Projektová rola:** | **MANAŽÉR KYBERNETICKEJ A INFORMAČNEJ BEZPEČNOSTI („KIB“)** |
| Stručný popis: | - má 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,  - má sprístupnené všetky informácie o bezpečnostných opatreniach zavádzaných projektom v zmysle § 20 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a v zmysle ustanovení zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,  - zodpovedá za posúdenie možných alternatív realizácie projektu za oblasť IB a KB,  - zodpovedá za posúdenie požiadaviek agendy IB a KB na rozhrania a spoločné komponenty, na integrácie a procesy konverzie a migrácie, identifikácia nesúladu a návrh riešenia,  - poskytuje konzultácie a súčinnosť pre problematiku IB a KB,  - poskytuje konzultácie pri tvorbe šablón a vzorov dokumentácie pre oblasť IB a KB,  - poskytuje konzultácie a vykonáva kontrolnú činnosť zameranú na obsah a komplexnosť dokumentácie z hľadiska IB a KB,  - dohliada na zosúladenie projektu s princípmi definovanými v interných riadiacich aktoch ÚV SR a dokumentoch týkajúcich sa bezpečnosti ÚV SR,  - zabezpečuje získavanie a spracovanie informácií nutných pre plnenie úloh v oblasti IB a KB,  - aktívne sa zúčastňuje stretnutí projektového tímu a spolupracuje na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Prílohou č.1 tejto smernice,  - plní pokyny PM a dohody zo stretnutí projektového tímu. |
| Detailný popis rozsahu zodpovedností, povinností a kompetencií | * zodpovedá́ za špecifikovanie: * štandardov, princípov a stratégií v oblasti informačnej bezpečnosti („IB“) a kybernetickej bezpečnosti („KB“) a ich dodržiavanie, * funkčných, nefunkčných a technických požiadaviek na IB a KB a za ich analýzu, * požiadaviek na IB a KB, kontroluje ich implementáciu v realizovanom projekte, * požiadaviek na bezpečnosť̌ vývojového, testovacieho a produkčného prostredia, * požiadaviek na bezpečnosť̌ v rámci bezpečnostnej vrstvy, * požiadaviek na školenia pre oblasť̌ IB a KB, * požiadaviek na bezpečnostnú́ architektúru riešenia a technickú́ infraštruktúru pre oblasť̌ IB a KB, * požiadaviek na dostupnosť̌, zálohovanie, archiváciu a obnovu IS vzťahujúce sa na IB a KB, * požiadaviek na IB a KB, bezpečnostný́ projekt a riadenie prístupu, * požiadaviek na opis vývojového, testovacieho a produkčného prostredia za oblasť̌ IB a KB, * požiadaviek na testovanie z hľadiska IB a KB, realizáciu kontroly zapracovania a retestu, * požiadaviek na obsah dokumentácie v zmysle legislatívnych požiadaviek pre oblasť̌ IB a KB, ako aj v zmysle "best practies", * požiadaviek na dodanie potrebnej dokumentácie súvisiacej s IBaKB kontroluje ich implementáciu v realizovanom projekte, * požiadaviek a konzultácie pri návrhu riešenia za agendu IB a KB v rámci procesu „Mapovanie a analýza technických požiadaviek - detailný́ návrh riešenia (DNR)“, * požiadaviek nabezpečnosť ITaKB v rámci procesu "akceptácie, odovzdania a správy zdrojových kódov“, * akceptačných kritérií́ za oblasť̌ IB a KB, * pravidiel pre publicitu a informovanosť̌ s ohľadom na IB a KB, * podmienok na testovanie, reviduje výsledky a výstupy z testovania za oblasť̌ IB a KB, * požiadaviek na bezpečnostný́ projekt pre oblasť̌ IB a KB, * zodpovedá́ za realizáciu kontroly: * zameranej na naplnenie požiadaviek definovaných v bezpečnostnom projekte za oblasť̌ IB a KB, * zameranú́ na správnosť̌ nastavení́ a konfigurácii bezpečnosti jednotlivých prostredí́, * zameranú́ na realizáciu procesu posudzovania a komplexnosti bezpečnostných rizík, bezpečnosť̌ a kompletný́ popis rozhraní́, správnu identifikácia závislostí, * naplnenia definovaných požiadaviek pre oblasť̌ IB a KB, * zameranú́ na implementovaný́ proces v priamom súvise s IB a KB, * súladu s platnou legislatívou v oblasti IB a KB (obsahuje aj kontrolu legislatívnych požiadaviek), * zameranú́ na zabezpečenie procesu, interfejsov, integrácii, kompletného popisu rozhraní́ a spoločných komponentov a posúdenia z pohľadu bezpečnosti, |

|  |  |
| --- | --- |
| **Projektová rola:** | **ČLEN PROJEKTOVÉHO TÍMU** |
| Stručný popis: | - vykonáva odbornú prácu v projekte a poskytuje odborné stanoviská a konzultácie za príslušnú oblasť,  - aktívne sa zúčastňuje odborných stretnutí tímu, ako aj konzultácií,  - zabezpečuje vypracovanie, priebežnú aktualizáciu a verzionovanie manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Prílohou č.1 tejto smernice v súčinnosti a podľa pokynov tímového manažéra a PM,  - plní úlohy uložené tímovým manažérom a PM v požadovanej kvalite a v stanovených termínoch,  - plní dohody zo stretnutí projektového tímu,  - odpočtuje plnenie úloh tímovému manažérovi a PM,  - predkladá námety, podnety, požiadavky a upozorňuje na problémy a riziká súvisiace s projektom tímovému manažérovi a PM,  - spolupracuje s projektovým tímom na strane dodávateľa,  - zodpovedá za splnenie všetkých legislatívnych požiadaviek (právne predpisy SR a EK) a metodických a administratívnych požiadaviek súvisiacich s implementáciou projektu. |

# Implementácia a preberanie výstupov projektu

Implementácia a preberanie výstupov projektu bude realizované v súlade s Vyhláškou Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 401/2023 Z. z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy v zmysle ustanovení podľa § 5 a nasledovných ustanovení.

# Prílohy

Koniec dokumentu