PROJEKTOVÝ ZÁMER

Manažérsky výstup I-02

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

|  |  |
| --- | --- |
| Povinná osoba | Slovenský pozemkový fond (SPF) |
| Názov projektu | Zvýšenie kybernetickej bezpečnosti v prostredí Slovenského pozemkového fondu |
| Zodpovedná osoba za projekt | Juraj Hušek |
| Realizátor projektu | Slovenský pozemkový fond (SPF) |
| Vlastník projektu | Slovenský pozemkový fond (SPF) |

Schvaľovanie dokumentu

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Položka** | **Meno a priezvisko** | **Organizácia** | **Pracovná pozícia** | **Dátum** | **Podpis**  **(alebo elektronický súhlas)** |
| Vypracoval | Juraj Hušek | SPF | Riaditeľ odboru |  |  |

# História DOKUMENTU

|  |  |  |  |
| --- | --- | --- | --- |
| **Verzia** | **Dátum** | **Zmeny** | **Meno** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE

V súlade s Vyhláškou č. 401/2023 Z.z. je dokument I-02 Projektový zámer určený na rozpracovanie detailných informácií prípravy projektu, aby bolo možné rozhodnúť o pokračovaní prípravy projektu, pláne realizácie, alokovaní rozpočtu a ľudských zdrojov.

Dokument Projektový zámer v zmysle vyššie uvedenej vyhlášky obsahuje manažérske zhrnutie, rozsah, ciele a motiváciu na realizáciu projektu, zainteresované strany, alternatívy, návrh merateľných ukazovateľov, detailný opis požadovaných projektových výstupov, detailný opis obmedzení, predpokladov, tolerancií a návrh organizačného zabezpečenia projektu, detailný opis rozpočtu projektu a jeho prínosov, náhľad architektúry a harmonogram projektu so zoznamom rizík a závislostí.

## Použité skratky a pojmy

|  |  |
| --- | --- |
| **SKRATKA/POJEM** | **POPIS** |
| EDR | Endpoint Detection and Response |
| GOVNET | Privátna sieť prevádzkované pre vládne inštitúcie organizáciou NASES |
| HW | Hardvér |
| IKT | Informačno-komunikačné technológie (organizácie) |
| IS | Informačný systém |
| METAIS | Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov |
| MIRRI SR | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky |
| NBÚ | Národný bezpečnostný úrad |
| OVM | Orgány verejnej moci |
| PPA | Pôdohospodárska platobná agentúra |
| SD | Service Desk |
| SIEM | Security information and event management |
| SLA | Service Level Agreement – dohoda/zmluva o parametroch poskytovania služby |
| SOAR | Security orchestration, automation and response |
| SPF | Slovenský pozemkový fond |
| SW | Softvér |
| XDR | Extended Detection and Response |

Tabuľka Zoznam skratiek

# DEFINOVANIE PROJEKTU

## Manažérske zhrnutie

Tento projekt je vypracovaný v súlade s vyhláškou č. 401/2023 Z. z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy.

Realizátorom projektu je Slovenský pozemkový fond, ktorý bol zriadený zákonom č. 330/1991 Zb. o pozemkových úpravách, usporiadaní pozemkového vlastníctva, pozemkových úradoch, pozemkovom fonde a o pozemkových spoločenstvách v znení neskorších predpisov a nie je zriadený na podnikanie.

Fond svoju činnosť vykonáva podľa vyššie citovaného zákona a osobitných predpisov (napr. zák. č. 229/1991 Zb. o úprave vlastníckych vzťahov k pôde a inému poľnohospodárskemu majetku v znení neskorších predpisov, zák. č. 180/1995 Z.z. o niektorých opatreniach na usporiadanie vlastníctva k pozemkom, zák. č. 181/1995 Z.z. o pozemkových spoločenstvách v znení neskorších predpisov, zák. č. 503/2003 Z.z. o navrátení vlastníctva k pozemkom v znení neskorších predpisov, zák. č. 161/2005 Z.z. o navrátení vlastníctva k nehnuteľným veciam cirkvám a náboženským spoločnostiam a o prechode vlastníctva k niektorým nehnuteľnostiam v znení neskorších predpisov) vo verejnom záujme a z tejto činnosti mu vznikajú práva a záväzky. Fond je právnickou osobou, ktorá sa zapisuje sa do obchodného registra, deň zápisu je 19.08.1991. SPF vykonáva svoju činnosť vo verejnom záujme.

V súlade s § 29 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „ZoKB“) prebehol v rámci SPF audit kybernetickej bezpečnosti. Predkladaný projekt nadväzuje na vykonaný audit a jeho cieľom je zabezpečiť realizáciu opatrení v nadväznosti zistenia auditu kybernetickej bezpečnosti.

Projektom budú dosiahnuté nasledovné kvantitatívne ako aj kvalitatívne prínosy. Kvantitatívne prínosy v rámci navrhovaného projektu spočívajú v znížení nákladov súvisiacich s odstraňovaním kybernetických incidentov.

Kvalitatívne prínosy v rámci navrhovaného projektu sú:

* Zníženie miery rizika vzniku kybernetického incidentu.
* Zvýšenie miery súladu s platnou legislatívou.
* Zvýšenie úrovne kybernetickej a informačnej bezpečnosti.
* Zvýšenie detekcie kybernetických bezpečnostných incidentov.
* Zvýšená dôvera používateľov.

Časový harmonogram projektu je nastavený na 18 mesiacov a finálnym termínom dokončenia do 31.12.2025. Začiatok projektu je naplánovaný od 07/2024 a má byť ukončený najneskôr do 12/2025. Následne v rámci prevádzky bude prebiehať podpora prevádzky. Podporné aktivity budú zabezpečované počas celých 18 mesiacov od začiatku trvania projektu.

Rámcový rozpočet projektu je stanovený na sumu 965 400 EUR s DPH, pričom cena vychádza z prieskumu trhu a projektov s obdobnými požiadavkami.

Projekt bude financovaný́ z rozpočtových prostriedkov SPF.

Projekt je v súlade s nasledovným typom aktivity: Podpora včasnej detekcie a zvýšenie schopnosti reakcie na kybernetické bezpečnostné incidenty a na adaptáciu najmodernejších technológií, na zvýšenie odolnosti základných služieb pred kybernetickými hrozbami, vrátane podpory inovatívnych produktov a služieb až po úroveň TRL 9 s definovanou hlavnou aktivitou: Realizácia opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti.

## Motivácia a rozsah projektu

V nasledujúcej časti sú popísané oblasti motivácie a rozsahu navrhovaného projektu.

### Problém, ktorý bude realizáciou projektu odstránený

V období v dňoch od 03.10.2023 do 15.11.2023 bol rámci SPF vykonaný audit kybernetickej bezpečnosti. Cieľom auditu kybernetickej bezpečnosti bolo overiť a posúdiť zhodu prijatých bezpečnostných opatrení a plnenie povinností podľa zákona č. 69/2018 Z. z. a súvisiacich osobitných predpisov vzťahujúcich sa na bezpečnosti sietí a informačných systémov prevádzkovateľa základnej služby, s požiadavkami podľa zákona, s cieľom zabezpečiť požadovanú úroveň kybernetickej bezpečnosti. Auditom kybernetickej bezpečnosti sa ďalej identifikovali nedostatky pri zabezpečovaní kybernetickej bezpečnosti prevádzkovateľom základnej služby, s cieľom prijať opatrenia na ich odstránenie, nápravu alebo predchádzanie.

Počas auditu bol identifikovaný nesúlad voči požiadavkám zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a súvisiacich vyhláškach. Výsledky auditu overenia súladu prevádzkovateľa základnej služby s požiadavkami zákona č. 69/2018 Z. z. a vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška č. 362/2018 Z. z.“) sú uvedené v nasledujúcej tabuľke:

|  |  |  |
| --- | --- | --- |
| Počet súladov | 28 | 9% |
| Počet čiastočných súladov: | 174 | 58% |
| Počet nesúladov: | 97 | 33% |
| Počet vyhodnotených: | **299** | **100%** |

Tabuľka Vyhodnotenie súladov kyber auditu

Ako preukazuje vyššie uvedená tabuľka z celkového počtu vyhodnotených povinností len v 9% poviností bol preukázaný súlad so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a súvisiacich vyhláškach. Akčný plán, ktorý tvorí prílohu k správe z auditu definuje kritické, vysoké a stredné opatrenia, ktoré budú naplnené aj reliazáciou tohto projektu a rovnako navrhovaný hafmonogram. Akčný plán z dôvodu jeho citlivosti a dôvernosti netvorí prílohu projektovej dokumentácie.

### Biznis procesy, ktoré sú predmetom projektu

Z pohľadu biznis procesov, účelom fondu je predovšetkým realizácia nasledovných aktivít:

* bezodplatný prevod z vlastníctva štátu do vlastníctva oprávnených osôb (reštituentov) nehnuteľnosti z dôvodu poskytovania reštitučných náhrad;
* bezodplatný prevod z vlastníctva štátu do vlastníctva cirkví a náboženských spoločností nehnuteľnosti odňaté v rozpore so zásadami demokratickej spoločnosti po preukázaní zákonom stanovených podmienok;
* odplatný prevod majetku na účely privatizácie;
* odplatný prevod nehnuteľností vo vlastníctve štátu na účely výstavby alebo ťažby;
* odplatný prevod nehnuteľností vo vlastníctve nezistených vlastníkov z dôvodov taxatívne uvedených v §19 ods. 3 zákona č. 180/1995 Z. z.;
* zámena a predaj pozemkov vo vlastníctve štátu, ako aj nadobúdanie pozemkov do vlastníctva štátu z dôvodov uvedených v nariadení vlády;
* predaj pozemkov a poskytovanie náhradných pozemkov na účely usporiadania vlastníctva v zriadených záhradných osadách;
* predaj pozemkov v pozemkových spoločenstvách (zákon č. 97/2013 Z.z.);
* zriaďovanie vecného bremena k pozemkom vo vlastníctve SR (§151n a nasl. Občiansky zákonník), a vo vlastníctve neznámych vlastníkov (§19 ods. 4 z. č. 180/1995 Z.z.);
* predaj pozemkov vo vlastníctve štátu podľa osobitných predpisov (priem. parky, významné investície);
* prenájom nehnuteľností na účely poľnohospodárstva alebo lesného hospodárstva, prípadne dočasne aj na iný účel podľa nariadenia vlády.

### Informácie o oblasti (OBSAH / AGENDA / ŽIVOTNÁ SITUÁCIA), ktorým sa projekt venuje

Z pohľadu životných situácií sa projekt venuje nasledovnej životnej situácii:

|  |  |  |
| --- | --- | --- |
|  | **Kód v číselníku (MetaIS)** | **Názov** |
| **Okruh životnej situácie** | B01 | Podpora podnikania |
| **Životná situácia** | 037 | Využívanie a ochrana pôdy |

Tabuľka Zoznam projektom zlepšovaných životných situácií

Výnos MF SR č. 478/2010 Z. z. o základnom číselníku úsekov verejnej správy a agend verejnej správy nedefinoval pre samotný SPF žiaden úsek. Avšak pre tento projekt je relevantný úsek U00067 Pozemkové úpravy a ochrana poľnohospodárskej pôdy. Tento úsek je takto naďalej vedený aj v centrálnom metainformačnom systéme verejnej správy (MetaIS) a to v súlade so zákonom o informačných technológiách vo verejnej správe č. 95/2019 Z. z. Úsek U00067 pozostáva z veľkého počtu agend, pričom agendy priamo relevantná pre projekt je uvedená v tabuľke nižšie. Ostatné agendy nie sú pre projekt relevantné, alebo sú relevantné len nepriamo.

|  |  |  |
| --- | --- | --- |
| **Kód v číselníku (MetaIS)** | **Názov agendy verejnej správy** | **Právny predpis, ktorým je agenda verejnej správy ustanovená** |
| A0000915 | Organizovanie vykonávania pozemkových úprav | Zákon č. 330/1991 Z. z. o pozemkových úpravách, usporiadaní pozemkového vlastníctva, pozemkových úradoch, pozemkovom fonde a o pozemkových spoločenstvách |
| A0000920 | Rozhodovanie o navrátení vlastníctva k pozemkom | Zákon č. 330/1991 Z. z. o pozemkových úpravách, usporiadaní pozemkového vlastníctva, pozemkových úradoch, pozemkovom fonde a o pozemkových spoločenstvách |

Tabuľka Zoznam agend relevantných pre projekt

### ROZSAH PROJEKTU

Realizátorom projektu je Slovenský pozemkový fond, ktorý bol zriadený zákonom č. 330/1991 Zb. o pozemkových úpravách, usporiadaní pozemkového vlastníctva, pozemkových úradoch, pozemkovom fonde a o pozemkových spoločenstvách v znení neskorších predpisov a nie je zriadený na podnikanie.

Projekt sa zameriava na oblasti, kde SPF identifikovalo najvyššiu mieru rizika a najvyššie dopady vyplývajúce z vykonaného auditu kybernetickej bezpečnosti v súlade s § 29 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Pri výbere opatrení SPF vychádzal najmä z požiadaviek určených zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej ako „zákon o KB“), zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení zákona č. 301/2023 Z. z. a príslušných vykonávacích právnych predpisov.

Súčasťou projektu sú nasledovné opatrenia vyplývajúce zo zrealizovaného auditu kybernetickej bezpečnosti:

|  |  |
| --- | --- |
| **Oblasť opatrení** | **Výstup projektu** |
| Organizácia kybernetickej a informačnej bezpečnosti | * Aktualizovaná bezpečnostnej dokumentácie vrátane rozsahu a spôsobu plnenia všeobecných bezpečnostných opatrení * Vypracovaná Stratégia a súvisiace bezpečnostné politiky |
| Riadenie rizík | * Identifikované informačné aktíva a implementovaný systém pre inventarizáciu aktív * Aktualizovaná metodika riadenia rizík nie je jednoznačná * Spracovaná analýza rizík |
| Personálna bezpečnosť | * Vypracovaný plán rozvoja bezpečnostného vzdelávania |
| Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami | * Vypracovaná analýzy rizík tretích strán a celého dodávateľského reťazca; * Vypracovaná analýza a posúdenie súladu všetkých aktuálnych zmlúv s tretími stranami so zákonom o KB a dobrou praxou; * Vypracovaný interný riadiaceho aktu upravujúci zásady kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami. |
| Bezpečnosť pri prevádzke informačných  systémov a sietí | * Vypracovaný interný riadiaci akt v oblasti riadenia zmien, riadenia kapacít, inštalácie softvéru v sieťach a informačných systémoch, inštalácia zariadení v sieťach a informačných systémoch, zaznamenávanie bezpečnostných záznamov a zaznamenávanie a vyhodnocovanie prevádzkových záznamov; |
| Hodnotenie zraniteľností  a bezpečnostné aktualizácie | * Vypracovaný interný riadiaci akt upravujúci proces riadenia implementácie bezpečnostných aktualizácií a záplat. |
| Sieťová a komunikačná bezpečnosť | * Vypracovaná kategorizácie sieti * Vypracovaná aktualizácia segmentácie sietí v súlade s pravidlami klasifikácie a kategorizácie; |
| Zaznamenávanie udalostí  a monitorovanie | * Implementovaný SIEM * Implementovaný XDR |
| Riešenie kybernetických bezpečnostných incidentov | * Vypracovaný interný riadiaci akt obsahujúceho a upravujúceho povinnosti týkajúce sa riešenia kybernetických bezpečnostných incidentov; |
| Kryptografické opatrenia | * Vypracovaný interný riadiaci akt upravujúci používanie kryptografických prostriedkov a šifrovania, vrátane vypracovania a dokumentácie systému správy kryptografických kľúčov a certifikátov |
| Kontinuita prevádzky | * Vypracovaný interný riadiaci akt obsahujúceho a upravujúci kontinuitu prevádzky následkom kybernetického bezpečnostného incidentu alebo inej krízovej situácie. |
| Audit a kontrolné činnosti | * Vypracovaný program posúdenia bezpečnosti na definované informačné technológie verejnej správy, hodnotenia zraniteľností a penetračných testov. |

Tabuľka Odporúčania na realizáciu

### MOTIVÁCIA PROJEKTU

SPF externým spôsobom realizoval audit kybernetickej bezpečnosti, ktorý mal preukázať správne prijatie opatrení vyplývajúcich z predchádzajúceho auditu. Audit však preukázal významné nedostatky, čo je s ohľadom na budúce zaradenie SPF medzi poskytovateľov základnej služby, akútnym problémom. Hlavnou motívaciou projektu je teda relizovanie nápravných opatrení a prostredníctvom nich zvýšenie a zlepšenie úrovne kybernetickej a informačnej bezpečnosti v rámci SPF.

|  |  |  |  |
| --- | --- | --- | --- |
| **Aktér** | **Cieľ** | **Požiadavka** | **Obmedzenie** |
| Slovenský pozemkový fond | Zvýšenie a zlepšenie úrovne kybernetickej a informačnej bezpečnosti v prostredí Slovenského pozemkového fondu.  Zaradenie Slovenského pozemkového fondu medzi poskytovateľov základnej služby. | Realizácia opatrení v nadväznosti na nedostatky vyplývajúce z auditu kybernetickej bezpečnosti. | Doteraz chýbajúca finančná podpora pre zavedenie opatrení. |
| Národný bezpečnostný úrad | Zvýšenie a zlepšenie úrovne kybernetickej a informačnej bezpečnosti v SR. | Kybernetická bezpečnosť ako základná súčasť verejnej správy. | - |
| MIIRI SR | Zvýšenie a zlepšenie úrovne kybernetickej a informačnej bezpečnosti vo verejnej správe. | Kybernetická bezpečnosť ako základná súčasť verejnej správy. | - |

Tabuľka Aktéri projektu, ich ciele, požiadavky a obmedzenia

A diagram of a company

Description automatically generated

Schéma Schéma 1: Motivácia stakeholderov projektu

Motiváciou je zároveň predísť možnému kybernetickému incidentu, ktorý by mohol mať závažné dopady, ako preukazuje vyhodnotenie identifikačných kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov podľa vyhlášky NBÚ č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov:

|  |  |  |
| --- | --- | --- |
| **Dopad kybernetického bezpečnostného incidentu v závislosti** | **Kategória** | **Vysvetlenie** |
| § 24 ods. 2 písm. a) zákona 69/2018 Z.z.  Počet používateľov základnej služby zasiahnutých kybernetickým bezpečnostným incidentom. | I. | Oblasť, ktorú navrhovaný projekt adresuje, sa dotýka:  350 zamestnancov  30 500 občanov, ktorí uskutočnili podanie  110 000 občanov, ktorí navštívili stránku SPF |
| § 24 ods. 2 písm. b) zákona 69/2018 Z.z.  Dĺžka trvania kybernetického bezpečnostného incidentu (čas pôsobenia kybernetického bezpečnostného incidentu)  a  § 24 ods. 2 písm. c) zákona  Geografické rozšírenie kybernetického bezpečnostného incidentu. § 24 ods. 2 písm. b) zákona 69/2018 Z.z. | I. | Pri predpokladanom závažnom kybernetickom incidente v trvaní 7 pracovných dní, by obmedzenie prevádzky bolo v rozsahu 19 600 hodín v rámci celej SR. (350 zamestnancov x 7 dní x 8 hodín) |
| § 24 ods. 2 písm. d) zákona 69/2018 Z.z.  Stupeň narušenia fungovania základnej služby. | III. | V prípade nefunkčnosti informačných systémov nie je k dispozícii náhradné riešenie. |
| § 24 ods. 2 písm. e) zákona 69/2018 Z.z.  Rozsah vplyvu kybernetického bezpečnostného incidentu na hospodárske alebo spoločenské činnosti štátu. | I. | Incident by spôsobil hospodársku stratu alebo hmotnú škodu najmenej jednému užívateľovi viac ako 250 000 eur. |

Tabuľka Dopad kybernetického bezpečnostného incidentu v závislosti

## Zainteresované strany/Stakeholderi

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **AKTÉR / STAKEHOLDER** | **SUBJEKT**  **(názov / skratka)** | **ROLA**  **(vlastník procesu/ vlastník dát/zákazník/ užívateľ …. člen tímu atď.)** | **Informačný systém**  **(MetaIS kód a názov ISVS)** |
| 1. | Ministerstvo investícií, regionálneho rozvoja a informatizácie SR | MIRRI | Gestor zákona č. 95/2019 Z. z. | Nerelevantné |
| 2. | Národný bezpečnostný úrad | NBÚ | Gestor zákona č. 69/2018 Z. z. | Nerelevantné |
| 3. | Slovenský pozemkový fond | GR ZVJS | Biznis vlastník | Nerelevantné |
| 5. | Organizačné útvary v rámci SPF | N/A | Kľúčový používateľ | Nerelevantné |

Tabuľka Zainteresované strany

## Ciele projektu

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Názov cieľa** | **Názov strategického cieľa** | **Spôsob realizácie strategického cieľa** |
| 01 | Zvýšenie a zlepšenie úrovne kybernetickej a informačnej bezpečnosti v prostredí Slovenského pozemkového fondu | Národná stratégia Kybernetickej bezpečnosti na roky 2021 – 2025:  4.1 Dôveryhodný štát pripravený na hrozby  4.4 Kybernetická bezpečnosť ako základná súčasť verejnej správy | zavedením funkčných procesov riadenia rizík kybernetickej bezpečnosti,  kontinuálne posilňovaním technických, organizačných a personálnych kapacít pre detekciu a riešenie kybernetických bezpečnostných incidentov na národnej úrovni a v rámci jednotlivých sektorov, vrátane kritickej infraštruktúry,  rozvojom schopností v oblasti detekcie a zberu bezpečnostne relevantných udalostí v národnom kybernetickom priestore, ako aj rozvoj schopností v oblasti vyhodnocovania udalostí a detekcie incidentov modernými technikami v národnom kybernetickom priestore uplatňovaním systematického prístupu ku kybernetickej bezpečnosti založeného na analýze a riadení rizík v každej dôležitej oblasti, pričom každá analýza musí vychádzať z plánu a metodiky jednotnej analýzy a riadenia rizík, zvýšením ochrany prevádzkovateľov základných služieb vo verejnej správe z hľadiska kybernetickej bezpečnosti tak, aby ich audit a pravidelné kontroly vykonávaných opatrení trvalo preukazovali pozitívny trend zlepšovania stavu kybernetickej bezpečnosti vo verejnej správe,  poskytovaním bezpečných a dostupných elektronických služieb štátu každému občanovi s umožnením plnohodnotného rovného využitia elektronických nástrojov, |

Tabuľka Ciele projektu

## Merateľné ukazovatele (KPI)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **ID/Názov cieľa** | **Názov ukazovateľa (KPI)** | **Popis ukazovateľa** | **Merná jednotka** | **AS IS merateľné hodnoty (aktuálne)** | **TO BE  Merateľné hodnoty (cieľové hodnoty)** | **Spôsob ich merania** | **Pozn.** |
| PO095 / PSKPSOI12 | 01 Zvýšenie a zlepšenie úrovne kybernetickej a informačnej bezpečnosti | Verejné inštitúcie podporované v  rozvoji kybernetických služieb,  produktov a procesov | Počet verejných inštitúcií, ktoré sú podporované za účelom rozvoja a modernizácie kybernetických služieb, produktov, procesov a zvyšovania vedomostnej úrovne napríklad v kontexte opatrení smerujúcich k elektronickej bezpečnosti verejnej správy. | verejné inštitúcie | 0 | 1 | Meta IS | N/A |
| PR017 / PSKPRCR11 | 01 Zvýšenie a zlepšenie úrovne kybernetickej a informačnej bezpečnosti | Používatelia nových a vylepšených  verejných digitálnych služieb,produktov a procesov | Počet používateľov nových a vylepšených  verejných digitálnych služieb,produktov a procesov | používatelia / rok | 0 | 350 | Meta IS | N/A |

Tabuľka KPIs projektu

## Špecifikácia potrieb koncového používateľa

Neaplikuje sa

## Riziká a závislosti

|  |  |  |  |
| --- | --- | --- | --- |
| **NÁZOV RIZIKA a ZÁVISLOSTI** | **POPIS RIZIKA a ZÁVISLOSTI** | **TYP KATEGÓRIE** | **DOPORUČENÉ RIEŠENIE MITIGAČNÉ OPATRENIE (návrh riešenia rizika / závislosti)** |
| Harmonogram projektu | Projekt nebude realizovaný v nastavenom časovom harmonograme. S tým súvisí aj riziko schopnosť dodávateľa dodať požadované tovary a služby načas | časové | Realizácia projektu bude riadená Riadiacim výborom projektu, ktorý bude zabezpečovať koordináciu projektu. Harmonogram projektu bol stanovený tak, aby umožnil riešiť prípadné problémy pri nasadení riešenia. |
| Implementačný tím | Implementačný tím nebude mať dostatočnú kapacitu, vedomosti a schopnosti | organizačné | Dodávateľ a interné implementačné tímy musia preukázať dostatočnú kapacitu, vedomosti a schopnosti pre realizáciu projektu a jeho výstupov. |
| Nedostatočné výstupy projektu | Riešenie nebude realizované v dostatočnej kvalite | organizačné | Výstupy manažérskych produktov pre riadenie projektu budú v súlade s dokumentom „Metodika riadenia QAMPR. |
| Nedostatočná spolupráca žiadateľa s dodávateľom | Z dôvodu nedostatočnej komunikácie alebo nedostatočnej dokumentácie nebude zabezpečené úpsešné zavedenie obstarávaných technológií | organizačné | Realizácia projektu bude riadená Riadiacim výborom projektu, ktorý bude zabezpečovať koordináciu projektu. |

Tabuľka Riziká a závislosti

## Stanovenie alternatív v biznisovej vrstve architektúry

Identifikovaným problémom je nízka miera súladu so zákonom č. 69/2018 Z.z. Keďže sa jedná o nesplnenie zákonných požiadaviek na biznisovej vrstve architektúry existuje len jedna možnosť, a to prijať opatrenia na splnenie zákonných požiadaviek. Napriek tomu nižšie sú načrtnuté 3 alternatívy na biznisovej vrstve.

Schéma Zvažované biznis alternatívy

|  |  |
| --- | --- |
| **Alternatíva** | **Stručný popis** |
| Alternatíva 1 | Prvou alternatívou je ponechanie súčasného stavu, t.j. bez intervencie a zabezpečenia súladu so zákonom č. 69/2018 Z.z.. |
| Alternatíva 2 | Vypracovanie a aktualizácia bezpečnostnej dokumentácie na základe zistení z vykonaného auditu kybernetickej bezpečnosti. V rámci druhej alternatívy by sa jednalo o vytvorenie chýbajúcej a aktualizáciu už vytvorenej ale nedostatočnej bezpečnostnej dokumentácie na základe zistení z vykonaného auditu kybernetickej bezpečnosti v súlade s legislatívnymi požiadavkami vyhlášky č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. |
| Alternatíva 3 | Tretia alternatíva zahŕňa vytvorenie chýbajúcej a aktualizáciu už vytvorenej ale nedostatočnej bezpečnostnej dokumentácie na základe zistení z vykonaného auditu kybernetickej bezpečnosti v súlade s legislatívnymi požiadavkami vyhlášky č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení a zároveň bude realizované zvýšenie úrovne kybernetickej a informačnej bezpečnosti prostredníctvom implementácie nástrojov XDR a SIEM. |

Tabuľka Popis alternatív

## Multikriteriálna analýza

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **KRITÉRIUM** | **ZDÔVODNENIE KRIÉRIA** | **STAKEHOLDER**  **1** | **STAKEHOLDER**  **2** | **STAKEHOLDER**  **3** |
| BIZNIS VRSTVA | Kritérium A Zabezpečenie súladu s platnou legislatívou (KO) | Keďže audit kybernetickej bezpečnosti identifikoval významné nedostatky, je nevyhnutné prijať v čo najkratšom čase príslušné opatrenia | X | X | X |
| Kritérium B Vytvorenie predpokladov pre splnenie požiadaviek kladených na PZS (KO) | Cieľom je zaradenie SPF medzi PZS (aj v súvislosti s novelou zákona 69/2018, s čím súvisia ďalšie povinnosti vzťahujúce sa na PZS | X | X | X |
| Kritérium C Zamedzenie kybernetickým incidentom (KO) | Okrem prijatia opatrení vo vzťahu k dokumentácii, riadiacim aktom a metodikám, je nevyhnutné predísť aj rizikám súvisiacim s chýbajúcimi nástrojmi ochrany pre kybernetickými incidentmi | X | X | X |

Tabuľka Kritéria pre MCA

**Vyhodnotenie MCA**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Zoznam kritérií** | **Alternatíva**  **1** | **Spôsob**  **dosiahnutia** | **Alternatíva 2** | **Spôsob**  **dosiahnutia** | **Alternatíva 3** | **Spôsob**  **Dosiahnutia** |
| Kritérium A | nie |  | áno | Alternatíva umožní zavedenie opatrení s cieľom zabezpečiť súlad s legislatívou | áno | Alternatíva umožní zavedenie opatrení s cieľom zabezpečiť súlad s legislatívou |
| Kritérium B | nie |  | áno | Alternatíva umožní vytvoriť podmienky pre zaradenie SPF medzi PZS | áno | Alternatíva umožní vytvoriť podmienky pre zaradenie SPF medzi PZS |
| Kritérium C | nie |  | Nie |  | áno | Alternatíva umožní predchádzať kybernetickým incidentom prostredníctvom zavedenia nástrojov XDR a SIEM |

Tabuľka Vyhodnotenie MCA

## Stanovenie alternatív v aplikačnej vrstve architektúry

Nie je relevantné pre projekt, nerealizuje sa nový ani sa nemení existujúci ISVS

## Stanovenie alternatív v technologickej vrstve architektúry

Alternatívy na úrovni technologickej architektúry reflektujú alternatívy vypracované na základe „nadradenej“ architektonickej aplikačnej vrstvy. Vzhľadom na to, že ide o implementáciu nástrojov na zvýšenie kybernetickej a informačnej bezpečnosti, je nutné tieto nástroje inštalovať, resp. implementovať v existujúcom technologickom prostredí a zariadeniach. Z tohto dôvodu je ekonomicky nevýhodné uvažovať s ďalšími alternatívami na technologickej vrstve architektúry.

# POŽADOVANÉ VÝSTUPY (PRODUKT PROJEKTU)

|  |
| --- |
| **Výstup projektu** |
| * Aktualizovaná bezpečnostnej dokumentácie vrátane rozsahu a spôsobu plnenia všeobecných bezpečnostných opatrení * Vypracovaná Stratégia a súvisiace bezpečnostné politiky |
| * Identifikované informačné aktíva a implementovaný systém pre inventarizáciu aktív * Aktualizovaná metodika riadenia rizík nie je jednoznačná * Spracovaná analýza rizík |
| * Vypracovaný plán rozvoja bezpečnostného vzdelávania |
| * Vypracovaná analýzy rizík tretích strán a celého dodávateľského reťazca; * Vypracovaná analýza a posúdenie súladu všetkých aktuálnych zmlúv s tretími stranami so zákonom o KB a dobrou praxou; * Vypracovaný interný riadiaceho aktu upravujúci zásady kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami. |
| * Vypracovaný interný riadiaci akt v oblasti riadenia zmien, riadenia kapacít, inštalácie softvéru v sieťach a informačných systémoch, inštalácia zariadení v sieťach a informačných systémoch, zaznamenávanie bezpečnostných záznamov a zaznamenávanie a vyhodnocovanie prevádzkových záznamov; |
| * Vypracovaný interný riadiaci akt upravujúci proces riadenia implementácie bezpečnostných aktualizácií a záplat. |
| * Vypracovaná kategorizácie sieti * Vypracovaná aktualizácia segmentácie sietí v súlade s pravidlami klasifikácie a kategorizácie; |
| * Implementovaný SIEM-SOAR * Implementovaný XDR |
| * Vypracovaný interný riadiaci akt obsahujúceho a upravujúceho povinnosti týkajúce sa riešenia kybernetických bezpečnostných incidentov; |
| * Vypracovaný interný riadiaci akt upravujúci používanie kryptografických prostriedkov a šifrovania, vrátane vypracovania a dokumentácie systému správy kryptografických kľúčov a certifikátov |
| * Vypracovaný interný riadiaci akt obsahujúceho a upravujúci kontinuitu prevádzky následkom kybernetického bezpečnostného incidentu alebo inej krízovej situácie. |
| * Vypracovaný program posúdenia bezpečnosti na definované informačné technológie verejnej správy, hodnotenia zraniteľností a penetračných testov. |

Tabuľka Výstupy projektu

# NÁHĽAD ARCHITEKTÚRY

## Biznis architektúra

Predmetom projektu nie sú biznis procesy ani biznis služby zabezpečované SPF. High level biznis architektúra je zobrazená na nasledujúcej schéme.

A diagram of a computer

Description automatically generated

Schéma Biznis architektúra

## Aplikačná architektúra

Predmetom projektu nie je zmena aplikačnej architektúry. Aplikačnú architektúru SPF tvoria:

1. **Kanály / Prístupové body**

* Webový portál
* Intranet

1. **Informačné systémy pre podporu koncových procesov**

Do tejto skupiny zaraďujeme informačné systémy slúžiace pre podporu hlavných agendových / koncových procesov slovenského pozemkového fondu (prenájmy, ROEP, prevody, reštitúcie, ...):

* Geografický informačný systém
* Depozit
* Právne akty

1. **Informačné systémy pre podporu podporných procesov**

Do tejto skupiny zaraďujeme informačné systémy slúžiace na podporu ekonomických, účtovníckych a HR procesov:

* Zverejňovanie objednávok a faktúr
* Účtovnícky program - ekonomický informačný systém
* Human
* Dochádzkový terminál
* Intranetový portál

1. **Externé / Podporné informačné systémy**

Tieto systémy rozdeľujeme na externé / podporné informačné systémy integrované na informačné systémy Slovenského pozemkového fondu alebo informačné systémy, ktoré nie sú integrované, ale sú používané pri vykonávaní rôznych procesov Slovenského pozemkového fondu:

* Katasterportal, Štátna pokladnica, Pošta, ÚPVS, Obchodný vestník MSSR, Finstat, Centrálny register zmlúv, OverSi

A screenshot of a diagram

Description automatically generated

Schéma Aplikačná architektúra

## Technologická architektúra

**Predmetom projektu nie je zmena technologickej architektúry**. Technologická architektúra SPF v súčasnosti zahŕňa:

* Celkový počet virtuálnych serverov vo virtuálnom prostredí  - 72 virtuálnych servrov + 31 testovacích staníc pre dané servre
* Celkový počet sieťových aktívnych prvkov - 30 aktívnych sieťových -  prvkov
* Celkový počet fyzických serverov (mimo virtuálneho prostredia) - 3 aktívne + 1 s Windows 10 na zálohovanie, a 3 vypnute
* Dostupná kapacita diskových polí - 80TB pre VM servre, 30TB pre VM vitual PC, 50TB NAS1, 50TB NAS2, 20TB zálohovací server GR1
* Celkový počet pracovných staníc - 506
* Celkový počet lokalít infraštruktúry - 21

Projekt nepredpokladá nákup HW vybavenia pre používateľov IS SPF. Schéma nižšie preukazuje spôsob riešenia technologickej architektúry v prostredí SPF, kedy časť aplikácií využíva infraštruktúrne služby vládneho cloudu a časť aplikácií infraštruktúru SPF. Zakreslené sú aj nové prvky, týkajúce sa bezpečnostnej architektúry v rámci infraštruktúrnych služieb SPF.

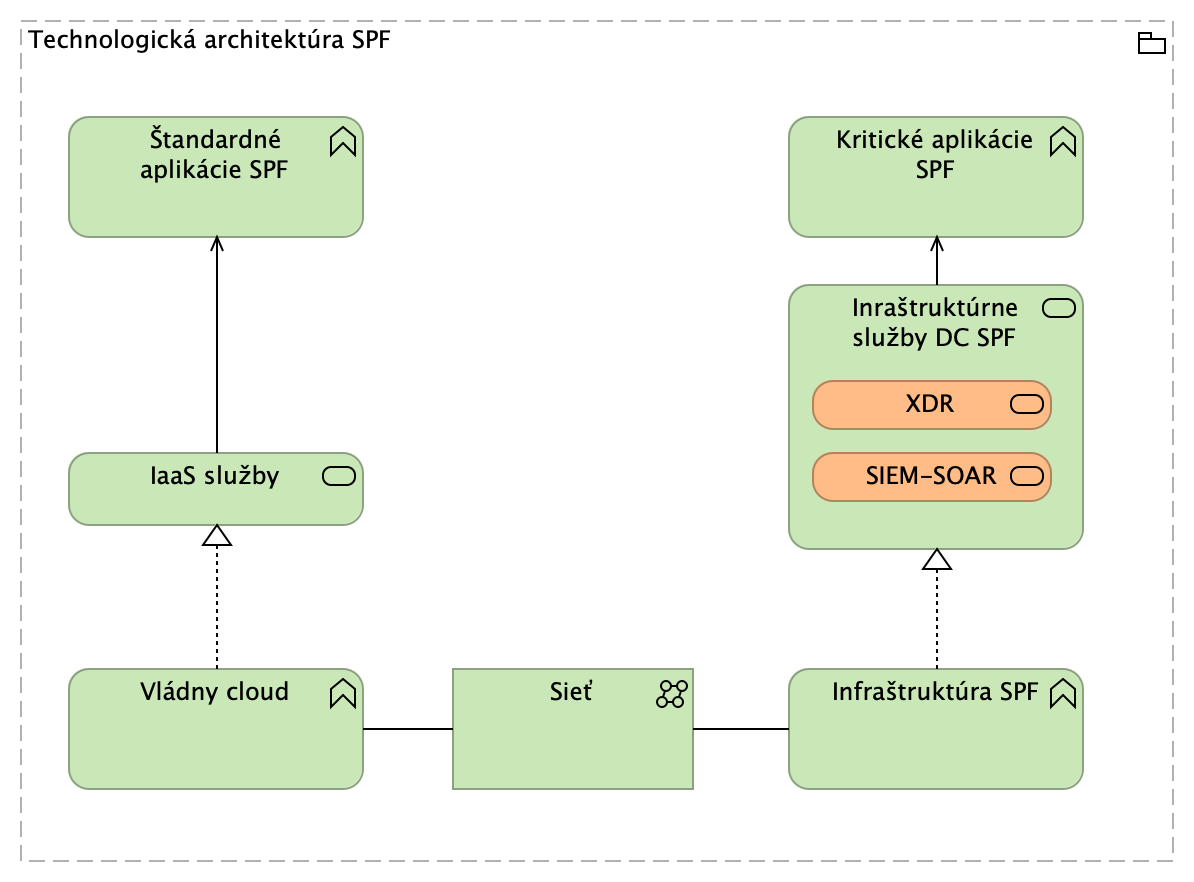


Schéma Technologická architektúra  – budúci stav

## Bezpečnostná architektúra

Navrhovaná bezpečnostná architektúra je v súlade s nasledovnými legislatívnymi normami:

* Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov,
* Zákon č. 95/2019 Z.z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov, ·
* 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 podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie 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.

Predmetom projektu sú nasledovné prvky bezpečnostnej architektúry:

1. Vypracovanie a aktualizácia dokumentácie na základe zistení auditu KB:

|  |  |
| --- | --- |
| **Oblasť opatrení** | **Výstup projektu** |
| Organizácia kybernetickej a informačnej bezpečnosti | * Aktualizovaná bezpečnostnej dokumentácie vrátane rozsahu a spôsobu plnenia všeobecných bezpečnostných opatrení * Vypracovaná Stratégia a súvisiace bezpečnostné politiky |
| Riadenie rizík | * Identifikované informačné aktíva a implementovaný systém pre inventarizáciu aktív * Aktualizovaná metodika riadenia rizík nie je jednoznačná * Spracovaná analýza rizík |
| Personálna bezpečnosť | * Vypracovaný plán rozvoja bezpečnostného vzdelávania |
| Riadenie kybernetickej a informačnej bezpečnosti vo  vzťahoch s tretími stranami | * Vypracovaná analýzy rizík tretích strán a celého dodávateľského reťazca; * Vypracovaná analýza a posúdenie súladu všetkých aktuálnych zmlúv s tretími stranami so zákonom o KB a dobrou praxou; * Vypracovaný interný riadiaceho aktu upravujúci zásady kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami. |
| Bezpečnosť pri prevádzke informačných  systémov a sietí | * Vypracovaný interný riadiaci akt v oblasti riadenia zmien, riadenia kapacít, inštalácie softvéru v sieťach a informačných systémoch, inštalácia zariadení v sieťach a informačných systémoch, zaznamenávanie bezpečnostných záznamov a zaznamenávanie a vyhodnocovanie prevádzkových záznamov; |
| Hodnotenie zraniteľností  a bezpečnostné aktualizácie | * Vypracovaný interný riadiaci akt upravujúci proces riadenia implementácie bezpečnostných aktualizácií a záplat. |
| Sieťová a komunikačná bezpečnosť | * Vypracovaná kategorizácie sieti * Vypracovaná aktualizácia segmentácie sietí v súlade s pravidlami klasifikácie a kategorizácie; |
| Riešenie kybernetických bezpečnostných incidentov | * Vypracovaný interný riadiaci akt obsahujúceho a upravujúceho povinnosti týkajúce sa riešenia kybernetických bezpečnostných incidentov; |
| Kryptografické opatrenia | * Vypracovaný interný riadiaci akt upravujúci používanie kryptografických prostriedkov a šifrovania, vrátane vypracovania a dokumentácie systému správy kryptografických kľúčov a certifikátov |
| Kontinuita prevádzky | * Vypracovaný interný riadiaci akt obsahujúceho a upravujúci kontinuitu prevádzky následkom kybernetického bezpečnostného incidentu alebo inej krízovej situácie. |
| Audit a kontrolné činnosti | * Vypracovaný program posúdenia bezpečnosti na definované informačné technológie verejnej správy, hodnotenia zraniteľností a penetračných testov. |

Tabuľka Zoznam opatrení

1. SIEM-SOAR. Správa bezpečnostných informácií a udalostí (SIEM) s nadväznou orchestráciou a automatizáciou riešení na vzniknuté incidenty (SOAR). Riešenie pre aktívny zber dát z monitorovaných zariadení a aplikácií v reálnom čase so schopnosťou ich analyzovania a identifikácie správania typického pre narušenie bezpečnosti s následnou automatizáciou bezpečnostných operácií a procesov reakcie na incidenty počas ich riešenia. Podrobný popis požiadaviek na SIEM-SOAR je uvedený v katalógu požiadaviek.

3) XDR –viacvrstvové integrované riešenie zabezpečenia koncových bodov, ktoré nepretržite monitoruje používateľské zariadenia. Riešenie umožní zhromažďovať údaje pomocou automatických reakcií založených na pravidlách. Platforma XDR zaznamenáva a vzdialene ukladá správanie koncových zariadení na úrovni systému. Potom ich analyzuje s cieľom odhaliť akúkoľvek podozrivú aktivitu a poskytnúť rôzne možnosti reakcie a obrany. Riešenie umožní 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. Podrobný popis požiadaviek na XDR je uvedený v katalógu požiadaviek.

# LEGISLATÍVA

Pre naplnenie cieľov a dodanie výstupov projektu nie sú potrebné zmeny v oblasti legislatívy.

# ROZPOČET A PRÍNOSY

Rozpočet projektu bol stanovený na základe premenných parametrov, ktorými boli nasledovné údaje:

* Celkový počet virtuálnych serverov vo virtuálnom prostredí - 72 virtuálnych servrov + 31 testovacích staníc pre dané servre
* Celkový počet sieťových aktívnych prvkov - 30 aktívnych sieťových - prvkov
* Celkový počet fyzických serverov (mimo virtuálneho prostredia) - 3 aktívne + 1 s Windows 10 na zálohovanie, a 3 vypnute
* Dostupná kapacita diskových polí - 80TB pre VM servre, 30TB pre VM vitual PC, 50TB NAS1, 50TB NAS2, 20TB zálohovací server GR1
* Celkový počet pracovných staníc – do 500
* Celkový počet lokalít infraštruktúry – 21

Na základe týchto parametrov bola stanovená výzvy na predkladanie indikatívnych cenových ponúk pre získanie informácie o Predpokladanej hodnote zákazky, pričom parametrizácia bola stanovená nasledovne (hodnoty počtu licencií pre SOAR a XDR vyšli rovnako z prieskumu na základe vecného vymedzenia projektu):

|  |  |  |  |
| --- | --- | --- | --- |
| **P.Č.** | **Položka** | **Počet** | **Merná jednotka** |
| 1 | Licencie pre SOAR, SIEM[1] | **32** | KS |
| 2 | [Licencie pre XDR[2]](file:///C:\\Users\\peter\\AppData\\Local\\Microsoft\\Windows\\INetCache\\Content.MSO\\9D88A3FD.xlsx" \l "RANGE!A14) | **28** | KS |
| 2 | HA riešenie | 1 | projekt |
| 3 | Analýza | 150 | MDs |
| 4 | Implementácia | 450 | MDs |
| 5 | Dokumentácia | 20 | MDs |
| 6 | Zaškolenie | 25 | MDs |

Tabuľka Parametrizácia projektu

V nasledujúcej tabuľke je vyhodnotenie PHZ z pohľadu dodávky a prevádzky diela:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | Spoločnosť 1 | Spoločnosť 2 | Spoločnosť 3 | **PRIEMER** |
| **P.Č.** | **Položka** | **Cena celkom s DPH** | **Cena celkom s DPH** | **Cena celkom s DPH** | **Cena celkom s DPH** |
| 1 | Dodanie služieb Kyber bezpečnosti | 560 640 € | 588 216 € | 581 174 € | 576 677 € |
| 2 | Prevádzka Kyber bezpečnosti | 365 880 € | 351 480 € | 341 520 € | 352 960 € |
| Spolu prevádzka | | 926 520 € | 939 696 € | 922 694 € | 929 637 € |

Tabuľka Vyhodnotenie PHZ

# HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU a METÓDA JEHO RIADENIA

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **FÁZA/AKTIVITA** | **ZAČIATOK**  **(odhad termínu)** | **KONIEC**  **(odhad termínu)** | **POZNÁMKA** |
| 1. | Prípravná fáza a Iniciačná fáza | 01/2024 | 10/2024 |  |
| 2. | Realizačná fáza | 10/2024 | 03/2026 |  |
| 2a | Analýza a Dizajn |  |  |  |
| 2b | Nákup technických prostriedkov, programových prostriedkov a služieb | 11/2024 | 04/2025 | Implementácia XDR a SIEM |
| 2c | Implementácia a testovanie | 11/2024 | 08/2025 |  |
| 2d | Nasadenie a PIP | 08/2025 | 01/2026 |  |
| 3. | Dokončovacia fáza | 02/2026 | 02/2026 |  |
| 4. | Podpora prevádzky (SLA) | 03/2026 | 02/2029 |  |

Tabuľka Harmonogram projektu

# PROJEKTOVÝ TÍM

Pre potreby riadenia projektu bude vytvorený riadiaci výbor projektu a vytvorený projektový tím prijímateľa. Riadiaci výbor projektu budú tvoriť minimálne nasledovní členovia, pričom na rokovania riadiaceho výboru budú podľa potreby prizývané iné osoby:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Meno a Priezvisko** | **Pozícia** | **Oddelenie** | **Rola v projekte** |
| **1.** | Tbc | Námestník GR | tbc | Predseda RV |
| **2.** | Tbc | Riaditeľ OIKT | tbc | Podpredseda RV - zástupca vlastníkov procesov |
| **3.** | Tbc | Manažér KB | tbc | zástupca kľúčových používateľov |
| **4.** | Tbc | tajomník RV | tbc | za SPF (bez hlasovacieho práva) |
| **5.** | tbc | projektový manažér | tbc | Projektový manažér za SPF (bez hlasovacieho práva) |

Tabuľka Zloženie riadiaceho výboru

Mená pre jednotlivé pozície projektového tímu budú doplnené pred zahájením realizačnej fázy projektu, na základe rozhodnutia riadiaceho výboru na základe návrhu projektového manažéra.

## PRACOVNÉ NÁPLNE

Predseda RV - Hlavným záujmom a zodpovednosťou predsedu Riadiaceho výboru projektu je:

* 1. zastupovať záujmy prijímateľa v projekte,
  2. kontrolovať súlad projektu a projektových cieľov so strategickými cieľmi,
  3. zabezpečiť a udržať finančné krytie (rozpočet) realizácie projektu,
  4. zabezpečiť nákladovo prijateľný prístup v projekte,

Podpredseda RV – zástupca vlastníkov procesov - Hlavným záujmom a zodpovednosťou zástupcu vlastníkov procesov (biznis vlastník) je:

* 1. schválenie funkčných a technických požiadaviek, potreby, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu,
  2. definovanie očakávaní na kvalitu projektu, kritérií kvality projektových produktov, prínosov pre koncových používateľov a požiadaviek na bezpečnosť,
  3. definovanie merateľných výkonnostných ukazovateľov projektov a prvkov,
  4. schválenie akceptačných kritérií,
  5. akceptáciu rozsahu a kvality dodávaných projektových výstupov pri dosiahnutí platobných míľnikov,
  6. odsúhlasenie spustenia výstupov projektu do produkčnej prevádzky,
  7. dostupnosť ľudských zdrojov alokovaných na realizáciu projektu

|  |  |
| --- | --- |
| **Projektová rola:** | **PROJEKTOVÝ MANAŽÉR** |
| **Stručný popis:** | * zodpovedá za riadenie projektu počas celého životného cyklu projektu. Riadi projektové (ľudské a finančné) zdroje, zabezpečuje tvorbu obsahu, neustále odôvodňovanie projektu (aktualizuje BC/CBA) a predkladá vstupy na rokovanie Riadiaceho výboru. Zodpovedá za riadenie všetkých (ľudských a finančných) zdrojov, členov projektovému tím objednávateľa a za efektívnu komunikáciu s dodávateľom alebo stanovených zástupcom dodávateľa. * zodpovedá za riadenie prideleného projektu - stanovenie cieľov, spracovanie harmonogramu prác, koordináciu členov projektového tímu, sledovanie dodržiavania harmonogramu prác a rozpočtu, hodnotenie a prezentáciu výsledkov a za riadenie s tým súvisiacich rizík. Projektový manažér vedie špecifikáciu a implementáciu projektov v súlade s firemnými štandardami, zásadami a princípmi projektového riadenia. * zodpovedá za plnenie projektových/programových cieľov v rámci stanovených kvalitatívnych, časových a rozpočtovým plánov a za riadenie s tým súvisiacich rizík. V prípade externých kontraktov sa vedúci projektu/ projektový manažér obvykle podieľa na ich plánovaní a vyjednávaní a je hlavnou kontaktnou osobou pre zákazníka. |
| **Detailný popis rozsahu zodpovednosti, povinností a kompetencií** | Zodpovedný za:   * Riadenie projektu podľa pravidiel stanovených vo Vyhláške 85/2020 Z.z. * Riadenie prípravy, inicializácie a realizácie projektu * Identifikovanie kritických miest projektu a navrhovanie ciest k ich eliminácii * Plánovanie, organizovanie, motivovanie projektového tímu a monitorovanie projektu * Zabezpečenie efektívneho riadenia všetkých projektových zdrojov s cieľom vytvorenia a dodania obsahu a zabezpečenie naplnenie cieľov projektu * Určenie pravidiel, spôsobov, metód a nástrojov riadenia projektu a získanie podpory Riadiaceho výboru (RV) pre riadenie, plánovanie a kontrolu projektu a využívanie projektových zdrojov * Zabezpečenie vypracovania manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 85/2020 Z.z., Prílohou č.1 * Zabezpečenie realizácie projektu podľa štandardov definovaných vo Vyhláške 78/2020 Z.z. * Zabezpečenie priebežnej aktualizácie a verzionovania manažérskej a špecializovanej dokumentácie v minimálnom rozsahu Vyhlášky 85/2020 Z.z., Prílohy č.1 * Vypracovanie, pravidelné predkladanie a zabezpečovanie prezentácie stavov projektu, reportov, návrhov riešení problémov a odsúhlasovania manažérskej a špecializovanej dokumentácie v rozsahu určenom Vyhláškou 85/2020 Z.z., Prílohou č.1 na rokovanie RV * Riadenie a operatívne riešenie a odstraňovanie strategických / projektových rizík a závislostí * Predkladanie návrhov na zlepšenia na rokovanie Riadiaceho výboru (RV) * Zabezpečenie vytvorenia a pravidelnej aktualizácie BC/CBA a priebežné zdôvodňovanie projektu a predkladanie na rokovania RV * Celkovú alokáciu a efektívne využívanie ľudských a finančných zdrojov v projekte * Celkový postup prác v projekte a realizuje nápravné kroky v prípade potreby * Vypracovanie požiadaviek na zmenu (CR), návrh ich prioritizácie a predkladanie zmenových požiadaviek na rokovanie RV * Riadenie zmeny (CR) a prípadné požadované riadenie konfigurácií a ich zmien * Riadenie implementačných a prevádzkových aktivít v rámci projektov. * Aktívne komunikuje s dodávateľom, zástupcom dodávateľa a projektovým manažérom dodávateľa s cieľom zabezpečiť úspešné dodanie a nasadenie požadovaných projektových výstupov, * Formálnu administráciu projektu, riadenie centrálneho projektového úložiska, správu a archiváciu projektovej dokumentácie * Kontrolu dodržiavania a plnenia míľnikov v zmysle zmluvy s dodávateľom, * Dodržiavanie metodík projektového riadenia, * Predkladanie požiadaviek dodávateľa na rokovanie Riadiaceho výboru (RV), * Vecnú a procesnú administráciu zúčtovania dodávateľských faktúr |
| **Odporúčané kvalifikačné predpoklady** | * Certifikácia - Prince 2 * Certifikácia - PMI PMP * Certifikácia - IPMA   Certifikát vydaný medzinárodne uznávanou akreditačnou a certifikačnou autoritou. |
| **Poznámka** | V prípade, ak v projektom tíme NIE SÚ vytvorené projektové role **Manažér zmien** (Change manager) a **Implementačný manažér** (Release manager), tak rozsah a povinnosti týchto rolí vykonáva rola **Projektový manažér** |

Tabuľka Popis pozície projektový manažér

|  |  |
| --- | --- |
| **Projektová rola:** | **KĽUČOVÝ POUŽIVATEĽ** (end user) |
| **Stručný popis:** | * zodpovedný za reprezentáciu záujmov budúcich používateľov projektových produktov alebo projektových výstupov a za overenie kvality produktu. * zodpovedný za návrh a špecifikáciu funkčných a technických požiadaviek, potreby, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu, požiadaviek koncových používateľov na prínos systému a požiadaviek na bezpečnosť. * Kľúčový používateľ (end user) navrhuje a definuje akceptačné kritériá, je zodpovedný za akceptačné testovanie a návrh na akceptáciu projektových produktov alebo projektových výstupov a návrh na spustenie do produkčnej prevádzky. Predkladá požiadavky na zmenu funkcionalít produktov a je súčasťou projektových tímov |
| **Detailný popis rozsahu zodpovednosti, povinností a kompetencií** | Zodpovedný za:   * Návrh a špecifikáciu funkčných a technických požiadaviek * Jednoznačnú špecifikáciu požiadaviek na jednotlivé projektové výstupy (špecializované produkty a výstupy) z pohľadu vecno-procesného a legislatívy * Vytvorenie špecifikácie, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu, * Špecifikáciu požiadaviek koncových používateľov na prínos systému * Špecifikáciu požiadaviek na bezpečnosť, * Návrh a definovanie akceptačných kritérií, * Vykonanie používateľského testovania funkčného používateľského rozhrania (UX testovania) * Finálne odsúhlasenie používateľského rozhrania * Vykonanie akceptačného testovania (UAT) * Finálne odsúhlasenie a akceptáciu manažérskych a špecializovaných produktov alebo projektových výstupov * Finálny návrh na spustenie do produkčnej prevádzky, * Predkladanie požiadaviek na zmenu funkcionalít produktov * Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 85/2020 Z.z., Prílohou č.1 * Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu |

Tabuľka Popis pozície kľúčový používateľ

|  |  |
| --- | --- |
| **Projektová rola:** | **MANAŽER KYBERNETICKEJ BEZPEČNOSTI (KIB) a IT BEZPEČNOSTI (ITB)** |
| **Stručný popis:** | * zodpovedá za dodržanie princípov a štandardov na kybernertickú a IT bezpečnosť, za kontrolu a audit správnosti riešenia v oblasti bezpečnosti. * koordinuje a riadi činnosť v oblasti bezpečnosti prevádzky IT, spolupracuje na projektoch, na rozvoji nástrojov a postupov k optimalizácii bezpečnostných systémov a opatrení. Stanovuje základné požiadavky, podmienky a štandardy pre oblasť bezpečnosti programov, systémov, databázy či sieti. Spracováva a kontroluje príslušné interné predpisy a dohliada nad plnením týchto štandardov a predpisov. Kontroluje a riadi činnosť nad bezpečnostnými testami, bezpečnostnými incidentmi v prevádzke IT. Poskytuje inštrukcie a poradenstvo používateľom počítačov a informačných systémov pre oblasť bezpečnosti   **PODMIENKY SPRÁVNEHO a EFEKTÍVNEHO VÝKONU ČINNOSTI role Manažér KIB a ITB:**   1. neobmedzený aktívny prístup ku všetkým projektovým dokumentom, nástrojom a výstupom projektu, v ktorých sa opisuje predmet projektu z hľadiska jeho architektúry, funkcií, procesov, manažmentu informačnej bezpečnosti a spôsobov spracúvania dát, ako aj dát samotných. 2. rola manažér Kybernetickej a IT bezpečnosti si vyžaduje mať sprístupnené všetky informácie o bezpečnostných opatreniach zavádzaných projektom v zmysle: 3. § 20 zákona č.69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov 4. ustanovení zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov |
| **Detailný popis rozsahu zodpovednosti, povinností a kompetencií** | Zodpovedný za:   * špecifikovanie štandardov, princípov a stratégií v oblasti ITB a KIB, * ak je projekt primárne zameraný na problematiku ITB a KIB – je priamo zodpovedný za špecifikáciu a analýzu funkčných požiadaviek na ITB a KIB, * špecifikovanie požiadaviek na ITB a KIB, kontroluje ich implementáciu v realizovanom projekte, * špecifikovanie požiadaviek na bezpečnosť vývojového, testovacieho a produkčného prostredia, * špecifikovanie funkčných a nefunkčných požiadaviek pre oblasť ITB a KIB, * špecifikovanie požiadaviek na bezpečnosť v rámci bezpečnostnej vrstvy, * špecifikovanie požiadaviek na školenia pre oblasť ITB a KIB, * špecifikovanie požiadaviek na bezpečnostnú architektúru riešenia a technickú infraštruktúru pre oblasť ITB a KIB, * špecifikovanie požiadaviek na dostupnosť, zálohovanie, archiváciu a obnovu IS vzťahujúce sa na ITB a KIB, * realizáciu posúdenie požiadaviek agendy ITB a KIB na integrácie a procesov konverzie a migrácie, identifikácia nesúladu a návrh riešenia * špecifikovanie požiadaviek na ITB a KIB, bezpečnostný projekt a riadenie prístupu, * špecifikovanie požiadaviek na testovanie z hľadiska ITB a KIB, realizáciu kontroly zapracovania a retestu, * špecifikovanie požiadaviek na obsah dokumentácie v zmysle legislatívnych požiadaviek pre oblasť ITB a KIB, ako aj v zmysle "best practies", * špecifikovanie požiadaviek na dodanie potrebnej dokumentácie súvisiacej s ITB a KIB kontroluje ich implementáciu v realizovanom projekte, * špecifikovanie požiadaviek a konzultácie pri návrhu riešenia za agendu ITB a KIB v rámci procesu „Mapovanie a analýza technických požiadaviek - detailný návrh riešenia (DNR)“, * špecifikáciu požiadaviek na bezpečnosť IT a KIB v rámci procesu "akceptácie, odovzdania a správy zdroj. kódov“ * špecifikáciu akceptačných kritérií za oblasť ITB a KIB, * špecifikáciu pravidiel pre publicitu a informovanosť s ohľadom na ITB a KIB, * poskytovanie konzultácií pri tvorbe šablón a vzorov dokumentácie pre oblasť ITB a KIB, * získavanie informácií nutných pre plnenie úloh v oblasti ITB a KIB, * špecifikáciu podmienok na testovanie, reviduje výsledky a výstupy z testovania za oblasť ITB a KIB, * konzultácie a vykonávanie kontrolnej činnosť zameranej na obsah a komplexnosť dok. z hľadiska ITB a KIB, * špecifikáciu požiadaviek na bezpečnostný projekt pre oblasť ITB a KIB, * realizáciu kontroly zameranej na naplnenie požiadaviek definovaných v bezp. projekte za oblasť ITB a KIB * realizáciu kontroly zameranú na správnosť nastavení a konfigurácii bezpečnosti jednotlivých prostredí, * realizáciu kontroly zameranú realizáciu procesu posudzovania a komplexnosti bezpečnostných rizík, bezpečnosť a kompletný popis rozhraní, správnu identifikácia závislostí, * realizáciu kontroly naplnenia definovaných požiadaviek pre oblasť ITB a KIB, * realizáciu kontroly zameranú na implementovaný proces v priamom súvise s ITB a KIB, * realizáciu kontroly súladu s planou legislatívou v oblasti ITB a KIB (obsahuje aj kontrolu leg. požiadaviek) * realizáciu kontroly zameranú zabezpečenie procesu, interfejsov, integrácii, kompletného popisu rozhraní a spoločných komponentov a posúdenia z pohľadu bezpečnosti, * poskytovanie konzultácií a súčinnosti pre problematiku ITB a KIB, * získavanie a spracovanie informácií nutných pre plnenie úloh v oblasti ITB a KIB, * aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 85/2020 Z.z., Prílohou č.1 * plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu |

Tabuľka Popis pozície manažér kyber bezpečnosti

# ODKAZY

N/A

# PRÍLOHY

Príloha 1: Zoznam rizík a závislostí

Príloha 2: Prístup k projektu – detailný

Príloha 3: Katalóg požiadaviek