MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

PROJEKTOVÝ ZÁMER

Manažérsky výstup P-02

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

Povinná osoba	Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky
Názov projektu	Zvýšenie úrovne kybernetickej a informačnej bezpečnosti Ministerstva školstva, výskumu, vývoja a mládeže Slovenskej republiky
Zodpovedná osoba za projekt	Mgr. Miroslav Odor
Realizátor projektu	Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky
Vlastník projektu	Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky

Schvaľovanie dokumentu

Položka	**Meno a priezvisko**	**Organizácia**	**Pracovná pozícia**	**Dátum**	**Podpis** (alebo elektronický súhlas)
Vypracoval	Mgr. Miroslav Odor	MŠVVaM SR			

1. HISTÓRIA DOKUMENTU

Verzia	**Dátum**	**Zmeny**	**Meno**
0.1	13.09.2024	Pracovný návrh	Mgr. Miroslav Odor
0.9	09.10.2024	Dokument - prípravná fáza	Mgr. Miroslav Odor

2. ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE

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

Dokument Projektový zámer bude v zmysle vyššie uvedenej vyhlášky a v zmysle výzvy: Zvýšenie úrovne kybernetickej a informačnej bezpečnosti, číslo výzvy: PSK-MIRRI-616-2024-DV-EFRR (ďalej len „výzva“), na základe ktorej má Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky (ďalej len „MŠVVaM SR“) záujem podať žiadosť o nenávratný finančný príspevok (ďalej len ŽoNFP), obsahovať: manažérske zhrnutie, motiváciu a rozsah projektu, zainteresované strany, ciele projektu a merateľné ukazovatele, návrh organizačného zabezpečenia projektu, alternatívy, opis obmedzení, predpokladov a tolerancií, opis požadovaných výstupov, náhľad architektúry, opis rozpočtu, detailný popis nákladov a prínosov, postup a spôsob nacenenia projektu, harmonogram projektu a zoznam rizík a závislostí (ako príloha projektového zámeru).

Manažérske produkty – vrátane projektového zámeru – sú s ohľadom na povahu dokumentov (verejne dostupné dokumenty) formulované tak, aby nešpecifikovali detailne konkrétne riziká a dopady a nezverejňovali podrobne dokumentáciu najväčších rizík IT systémov. Uvádzajú iba oblasti identifikovaných rizík a dopadov.

2.1 Použité skratky a pojmy

SKRATKA/POJEM	**POPIS**
ESVRŠ	Portál elektronických služieb regionálneho a vysokého školstva
IČO	Identifikačné číslo organizácie
IS	Informačný systém resp. informačné systémy
ISVS	Informačný systém verejnej správy
IT	Informačné technológie
KIB	Kybernetická a informačná bezpečnosť
NBÚ	Národný bezpečnostný úrad
MŠVVaM SR	Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky

OVM	Orgán verejnej moci
PZS	Poskytovateľ základnej služby (základných služieb)
RIS	Rezortný informačný systém
VŠ	Vysoká škola
Výzva	Výzva s názvom: „Zvýšenie úrovne kybernetickej a informačnej bezpečnosti", kód výzvy: PSK-MIRRI-616-2024-DV-EFRR
Zákon o ITVS	Zákon 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
ZS	Základná služba (základné služby)

2.2 Konvencie pre typy požiadaviek (príklady)

V rámci projektu budú definované tri základné typy požiadaviek:

Funkčné (používateľské) požiadavky majú nasledovnú konvenciu:

FPXX_MOD_XX

- F – funkčná požiadavka
- XX – číslo požiadavky
- MOD – označenie modulu
- XX – číslo modulu

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

Nxx

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

Technické požiadavky majú nasledovnú konvenciu:

Txx

- T – technická požiadavka
- xx – číslo požiadavky

3. DEFINOVANIE PROJEKTU

3.1 Manažérske zhrnutie

MŠVVaM SR má ku dňu spracovania projektového zámeru realizovaný audit kybernetickej bezpečnosti, ktorý bol vypracovaný (na základe overení) v decembri 2023. Z auditu kybernetickej bezpečnosti vyplynuli nasledovné skutočnosti:

Celková úroveň riadenia kybernetickej bezpečnosti MŠVVaM SR v zmysle požiadaviek zákona o kybernetickej bezpečnosti, vyhlášky 362/2018 Z.z. a implementovaných opatrení KIB na MŠVVaM SR je na 54% v súlade so zákonnými požiadavkami. MŠVVaM SR ako PZS vykonáva procesy na základe dokumentácie, v zmysle požiadaviek vyhlášky č. 362/2018 Z. z. Vyhláška Národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

Najvyššia miera nesúladu s legislatívnymi požiadavkami vyplývajúca z auditu kybernetickej bezpečnosti bola identifikovaná v nasledovných oprávnených oblastiach v zmysle výzvy:

- Riadenie prístupov
- Bezpečnosť pri prevádzke informačných systémov a sietí
- Ochrana proti škodlivému kódu
- Sieťová a komunikačná bezpečnosť
- Zaznamenávanie udalostí a monitorovanie
- Riešenie kybernetických bezpečnostných incidentov
- Zabezpečenie kontinuity prevádzky
- Audity a kontrolné činnosti

V uvedených oblastiach je potrebné realizovať nasledovné opatrenia KIB na zvýšenie súladu opatrení KIB s príslušnou legislatívou:

- Zavedenie správy privilegovaných účtov
- Zavedenie aplikácie na správu a aktualizáciu bezpečnostnej dokumentácie
- Zabezpečenie ochrany užívateľských zariadení pred kybernetickými hrozbami
- Zabezpečenie ochrany serverov pred kybernetickými hrozbami
- Zlepšenie sieťovej a komunikačnej bezpečnosti
- Rozšírenie logovacieho systému o korelácie a automatizáciu
- Implementácia podporných systémov pre zabezpečenie kontinuity prevádzky
- Zavedenie infraštruktúry pre prevádzku kybernetickej bezpečnosti a informačnej bezpečnosti

- Audity kybernetickej bezpečnosti
    - audit v roku 2025 (pravidelný)
    - audit pri ukončení projektu (mimoriadny)

Hlavným problémom, ktorému MŠVVaM SR ako PZS čelí, je teda vyriešenie vyššie pomenovaných oblastí informačnej a kybernetickej bezpečnosti tak, aby bol dosiahnutý maximálny možný súlad v oblasti príslušných predpisov KIB, a súčasne, aby boli administratívne a technologické náležitosti KIB realizované tak, aby chránili IT systémy, ktoré zabezpečujú prevádzku základných služieb pred kybernetickými útokmi, plnili svoje úlohy počas implementácie i v čase udržateľnosti projektu, boli pripravené na ďalší rozvoj IT technológií PZS, bolo možné ich flexibilne rozširovať bez ohrozenia prevádzkovaných i budúcich IT systémov.

Ciele projektu:

- Zavedenie správy privilegovaných účtov
- Zavedenie aplikácie na správu a aktualizáciu bezpečnostnej dokumentácie
- Zabezpečenie ochrany užívateľských zariadení pred kybernetickými hrozbami
- Zabezpečenie ochrany serverov pred kybernetickými hrozbami
- Zlepšenie sieťovej a komunikačnej bezpečnosti
- Rozšírenie logovacieho systému o korelácie a automatizáciu
- Implementácia podporných systémov pre zabezpečenie kontinuity prevádzky
- Zavedenie infraštruktúry pre prevádzku kybernetickej bezpečnosti a informačnej bezpečnosti
- Audity kybernetickej bezpečnosti

Cieľová skupina – správcovia IT systémov MŠVVaM SR, zamestnanci, verejnosť, podnikateľské subjekty poskytujúce IT služby MŠVVaM SR, a OVM, ktoré spolupracujú s MŠVVaM SR.

Realizáciou aktivít projektu dosiahne MŠVVaM SR naplnenie hlavného cieľa, ktorým je zvýšenie úrovne kybernetickej bezpečnosti a zabezpečenia prevádzky informačných systémov a sietí.

Projekt je v súlade s intervenčnou stratégiou Programu Slovensko 2021-2027 v nasledovných oblastiach:
1) súlad projektu so špecifickým cieľom: RSO1.2 (opatrenie 1.2.1)
2) súlad s očakávanými výsledkami definovanými v Partnerskej dohode pre špecifický cieľ RSO 1.2
3) súlad s definovanými typmi oprávnených aktivít v rámci výzvy.

Realizáciou projektu budú naplnené nasledovné merateľné ukazovatele:

PO095 / PSKPSOI12 – cieľová hodnota 1

PR017 / PSKPRCR11 – cieľová hodnota 700

Miesto realizácie:

Slovenská republika.

Predpokladaný rozpočet projektu (oprávnených výdavkov) je **maximálne 3 000 000** EUR (presná hodnota bude stanovená v inciačnej fáze projektu).

Sumarizácia hlavných parametrov hodnotenia predkladaného hodnotenia projektu:

- implementácia nástrojov pre zavedenie zálohovania na obnovu siete a informačného systému vrátane pravidelného testovania obnovy záloh **(predpoklad získania 8 bodov)**
- implementácia nástrojov pre manažment konfigurácií počítačových sietí a IT aktív, zoznam ich vlastníkov/správcov, vzájomných väzieb, súvisiacej dokumentácie a zoznam a opis prostredí, v ktorom sú aktíva umiestnené a prevádzkované (tzv. CMDB), ktorý sa viaže na inventarizáciu IT aktív **(predpoklad získania 9 bodov)**
- implementácia nástrojov na manažment zraniteľností kybernetickej bezpečnosti a riadenie záplat a aktualizácií za účelom zabezpečiť konzistentné nasadzovanie potrebných softvérových opráv a aktualizácií **(predpoklad získania 10 bodov)**
- implementácia nástrojov pre zavedenie viac-faktorovej autentifikácie **(predpoklad získania 7 bodov)**
- implementácia nástrojov pre zavedenia manažmentu mobilných zariadení **(predpoklad získania 5 bodov)**
- implementácia nástrojov, ktorých cieľom je zvýšiť schopnosť detekcie škodlivých aktivít a bezpečnostných incidentov, resp. ochrana koncových bodov, dát, dátových prenosov a sieťovej komunikácie, alebo ktorých cieľom je zvýšenie ochrany pred kybernetickými útokmi z externého prostredia **(predpoklad získania 11 bodov)**

- Miera rizík ohrozujúcich úspešnú realizáciu projektu (menej ako 10 % rizík z celkového počtu identifikovaných rizík v ŽoNFP je s vysokou závažnosťou, ktoré ohrozujú úspešnú realizáciu projektu **– predpoklad získania 20 bodov**)

- Administratívne, odborné a prevádzkové kapacity žiadateľa (Žiadateľ disponuje a plánuje (v súlade s podmienkami výzvy) dostatočné odborné kapacity s náležitou odbornou spôsobilosťou a know-how na riadenie a implementáciu projektu v danej oblasti. Popis zabezpečenia prevádzky riešenia je reálny, t. j. žiadateľ disponuje a plánuje (v súlade s podmienkami výzvy) personálne kapacity pre zabezpečenie prevádzky riešenia **– predpoklad získania 10 bodov**)

- Miera oprávnenosti výdavkov projektu (výška neoprávnených výdavkov medzi 0 % a 7 % (vrátane) – **predpoklad získania 20 bodov**).

3.2 Motivácia a rozsah projektu

MŠVVaM SR je právnickou osobou (IČO: 00164381) zapísanou v registri organizácií vedenom Štatistickým úradom Slovenskej republiky v zmysle § 3 ods. 1 písmena a) zákona č. 523/2004 Z. z. o rozpočtových pravidlách verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, t.j. ide o subjekt vo verejnej správe, konkrétne ústrednej správe. Zároveň je MŠVVaM SR zaradené v registri prevádzkovateľov základných služieb podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon o kybernetickej bezpečnosti“) v sektore verejná správa (viď: https://www.nbu.gov.sk/7276-sk/zoznam-zakladnych-sluzieb/), t.j. je poskytovateľom základnej služby (ďalej len PZS). MŠVVaM SR poskytuje nasledovné základné služby:

- Centrálna elektronická prihláška na vysoké školy
- RIS - Rezortný informačný systém
- Centrálny register zamestnancov VŠ
- Centrálny register študentov vysokých škôl
- Portál Ministerstva školstva, vedy, výskumu a športu SR

Pripravuje sa zavedenie dvoch ďalších základných služieb:

- Portál elektronických služieb regionálneho a vysokého školstva (ESVRŠ)
- Účtovný systém „Sofia“,

ktoré budú chránené opatreniami zavedenými v rámci tohto projektu.

Z uvedeného vyplýva o.i. skutočnosť, že MŠVVaM SR má povinnosť realizovať a financovať opatrenia kybernetickej a informačnej bezpečnosti (ďalej len KIB) definované najmä v zákonoch o kybernetickej bezpečnosti a v zákone 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ITVS“) a ďalších súvisiacich predpisoch.

3.2.1 Hlavný popis problému

MŠVVaM SR má ku dňu spracovania projektového zámeru realizovaný audit kybernetickej bezpečnosti, ktorý bol vypracovaný (na základe overení) v decembri 2023. Z auditu kybernetickej bezpečnosti vyplynuli nasledovné skutočnosti:

Celková úroveň riadenia kybernetickej bezpečnosti MŠVVaM SR v zmysle požiadaviek zákona o kybernetickej bezpečnosti, vyhlášky 362/2018 Z.z. a implementovaných opatrení KIB na MŠVVaM SR je na 54% v súlade so zákonnými požiadavkami. MŠVVaM SR ako PZS vykonáva procesy na základe dokumentácie, v zmysle požiadaviek vyhlášky č. 362/2018 Z. z. Vyhláška Národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

Najvyššia miera nesúladu s legislatívnymi požiadavkami vyplývajúca z auditu kybernetickej bezpečnosti bola identifikovaná v nasledovných oprávnených oblastiach v zmysle výzvy:

- Riadenie prístupov
- Bezpečnosť pri prevádzke informačných systémov a sietí
- Ochrana proti škodlivému kódu
- Sieťová a komunikačná bezpečnosť
- Zaznamenávanie udalostí a monitorovanie
- Riešenie kybernetických bezpečnostných incidentov
- Zabezpečenie kontinuity prevádzky
- Audity a kontrolné činnosti

V uvedených oblastiach je potrebné realizovať nasledovné opatrenia KIB na zvýšenie súladu opatrení KIB s príslušnou legislatívou:

- Zavedenie správy privilegovaných účtov
- Zavedenie aplikácie na správu a aktualizáciu bezpečnostnej dokumentácie
- Zabezpečenie ochrany užívateľských zariadení pred kybernetickými hrozbami
- Zabezpečenie ochrany serverov pred kybernetickými hrozbami
- Zlepšenie sieťovej a komunikačnej bezpečnosti
- Rozšírenie logovacieho systému o korelácie a automatizáciu
- Implementácia podporných systémov pre zabezpečenie kontinuity prevádzky
- Zavedenie infraštruktúry pre prevádzku kybernetickej bezpečnosti a informačnej bezpečnosti
- Audity kybernetickej bezpečnosti
    - audit v roku 2025 (pravidelný)
    - audit pri ukončení projektu (mimoriadny)

Ako vyplýva z vyššie uvedeného, hlavným **problémom, ktorému MŠVVaM SR ako PZS čelí, je teda vyriešenie vyššie pomenovaných oblastí informačnej a kybernetickej bezpečnosti tak, aby bol dosiahnutý maximálny možný súlad v oblasti príslušných predpisov KIB, a súčasne, aby boli administratívne a technologické náležitosti KIB realizované tak, aby:**

- **chránili IT systémy, ktoré zabezpečujú prevádzku základných služieb pred kybernetickými útokmi**
- **plnili svoje úlohy počas implementácie i v čase udržateľnosti projektu**
- **boli pripravené na ďalší rozvoj IT technológií PZS**
- **a bolo možné ich flexibilne rozširovať bez ohrozenia prevádzkovaných i budúcich IT systémov.**

3.2.2 Biznis procesy

Predmetom realizácie projektu bude zavedenie alebo aktualizácia a IT podpora nasledovných biznis procesov:

- Riadenie prístupov
- Riadenie prevádzky informačných systémov a sietí
- Ochrana proti škodlivému kódu
- Riadenie sieťovej a komunikačnej bezpečnosti
- Zaznamenávanie, monitorovanie a riešenie incidentov kybernetickej bezpečnosti
- Zabezpečovanie kontinuity prevádzky
- Vykonávanie auditu a kontrolných činností
- Zabezpečovanie prevádzky opatrení KIB

Realizáciou projektu nesmú byť narušené existujúce procesy KIB, ktoré projektom nebudú dotknuté.

Okrem samotného zabezpečenia opatrení KIB v zmysle zákona o kybernetickej bezpečnosti a zákona o ITVS a podporou vyššie uvedených biznis procesov sa projekt bude dotýkať prakticky všetkých biznis procesov, ktoré sú vykonávané MŠVVaM SR ako PZS, a ktoré sú realizované prostredníctvom informačných systémov MŠVVaM SR za účelom poskytovania základných služieb.

3.2.3 Oblasti zamerania projektu

Projekt sa primárne zaoberá oblasťou zabezpečenia opatrení KIB v zmysle zákona o kybernetickej bezpečnosti, zákona o ITVS a vyhlášky 326/2018 Z. z.. Ako bude uvedené ďalej, tento projekt má priamy dopad na všetky ISVS a technologické platformy (viď prístup k projektu), ktoré sú určené na poskytovanie základnej služby (resp. základných služieb) MŠVVaM SR, nakoľko výsledky projektu budú ochraňovať všetky tieto IS pred potenciálnymi hrozbami kybernetickej a informačnej bezpečnosti.

3.2.4 Rozsah projektu

Realizácia projektu sa dotkne nasledovných ISVS prevádzkovaných na úrovni MŠVVaM SR:

1. isvs_376 Centrálna elektronická prihláška na vysoké školy
2. isvs_6092 RIS - Rezortný informačný systém
3. isvs_6712 Centrálny register zamestnancov VŠ
4. isvs_374 Centrálny register študentov vysokých škôl
5. isvs_6301 Portál Ministerstva školstva, vedy, výskumu a športu SR (WEB)

Uvedené ISVS sú technologicky prevádzkované prostredníctvom 17 samostatných softvérových technológií (informačných systémov). .

Realizácia projektu sa dotkne nasledovných subjektov:

- MŠVVaM SR ako PZS
- Interní zamestnanci MŠVVaM SR
- Občania, podnikatelia a iné subjekty využívajúce základné služby MŠVVaM SR
- IS externých subjektov, ktoré sú poskytované ako služba pre MŠVVaM SR
- IS externých subjektov, ktoré využívajú služby ISVS MŠVVaM SR, ktoré sú predmetom ochrany opatreniami KIB realizovanými v rámci projektu

3.2.5 Motivácia a obmedzenia pre dosiahnutie cieľov projektu

Hlavnou motiváciou je realizácia opatrení KIB definovaných v zákone o kybernetickej bezpečnosti a v zákone o ITVS. **Vďaka realizácii týchto opatrení budú IS MŠVVaM SR** (a to primárne tie, ktoré zabezpečujú prevádzku základných služieb) **chránené v maximálnej možnej miere pred kybernetickým incidentom, ktorý by mohol mať na IS MŠVVaM SR nasledovný dopad:**

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.	II.	Počet interných zamestnancov ku dňu prípravy projektu: 722 zamestnancov TPP 216 zamestnancov na dohodu o vykonaní práce alebo dohody o pracovnej činnosti Počet klientov (používateľov základných služieb):

		• Centrálna elektronická prihláška na vysoké školy – počet používateľov 4233 • RIS - Rezortný informačný systém – pristupuje 6900 škôl resp. zriaďovateľov • Centrálny register zamestnancov VŠ – počet používateľov 64 • Centrálny register študentov vysokých škôl – počet používateľov 384 • Portál Ministerstva školstva, vedy, výskumu a športu SR – počet prístupov 10,8 mil./ročne Celkový dotknutý počet osôb potenciálne dotknutých jedným KIB môže byť na úrovni viac ako 50 000 osôb a menej ako 100 000 osôb.
§ 24 ods. 2 písm. b) zákona 69/2018 Z.z. Dĺžka trvania kybernetického bezpečnostného incidentu (čas pôsobenia kybernetického bezpečnostného incidentu) a/alebo § 24 ods. 2 písm. c) zákona Geografické rozšírenie kybernetického bezpečnostného incidentu.	II.	MŠVVaM SR má 5 ISVS určených na prevádzku ZS, ktoré sú technicky realizované pomocou 17 IS. V prípade kybernetického incidentu predpokladáme nedostupnosť IS na maximálne 10 pracovných dní, čo by v praxi znamenalo obmedzenie alebo narušenie prevádzky základnej služby: • v rozsahu 54150,00 hodín pre TPP zamestnancov MŠVVaM SR (10x722x7,5 - pracovný čas je 7,5 hodiny) • v rozsahu 4320,00 hodín pre zamestnancov zamestnaných na dohodu (predpokladáme prácu 2 hodiny denne t.j. 216x10x2) • v rozsahu 5 hodín hodín pre používateľov ZS „Centrálna elektronická prihláška na vysoké školy ((4233/8766)x10; 8766 je počet hodín v roku) • v rozsahu 138000 hodín pre používateľov ZS „Rezortný informačný systém“ – predpokladáme využívanie používateľmi 2 hodiny denne, t.j. 6900 x 2 x 10 • v rozsahu 640 hodín pre používateľov ZS „Centrálny register zamestnancov VŠ“ – predpokladáme využívanie používateľmi 1 hodinu denne, t.j. 64 x 1 x 10 • v rozsahu 3840 hodín pre používateľov ZS „Centrálny register študentov vysokých škôl“ – predpokladáme využívanie používateľmi 1 hodinu denne t.j. 384 x 1 x 10 • v rozsahu 12320,00 hodín pre používateľov ZS „Portál Ministerstva školstva, vedy, výskumu a športu SR“ ak predpokladáme, že pri prístupe používateľ využíva služby portálu jednu hodinu ((10800000/8766)*10) Celkovo teda v prípade KIB bude dopad v rozsahu 213275 používateľských hodín.

		Dopad KIB bude na úrovni celého územia Slovenskej republiky.
§ 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.	II.	V prípade nefunkčnosti bude zasiahnutých priamo 938 pracovníkov MŠVVaM SR a minimálne 23901 používateľov ZS MŠVVaM SR. Predpokladaná hospodárska jednému užívateľovi, konkrétne uvádzame stratu MŠVVaM SR na úrovni strát interných finančných prostriedkov – môže byť vyčíslená na viac ako 680006,10 EUR.

Okrem eliminácie dopadov uvedených v tabuľke vyššie sú motiváciou realizácie projektu činnosti nadväzujúce na odstraňovanie najvyššej miery nesúladu podľa auditu kybernetickej bezpečnosti (viď kapitola 3.2.1):

- implementácia nástrojov pre zavedenie zálohovania na obnovu siete a informačného systému vrátane pravidelného testovania obnovy záloh
- implementácia nástrojov pre manažment konfigurácií počítačových sietí a IT aktív, zoznam ich vlastníkov/správcov, vzájomných väzieb, súvisiacej dokumentácie a zoznam a opis prostredí, v ktorom sú aktíva umiestnené a prevádzkované (tzv. CMDB), ktorý sa viaže na inventarizáciu IT aktív
- implementácia nástrojov na manažment zraniteľností kybernetickej bezpečnosti a riadenie záplat a aktualizácií za účelom zabezpečiť konzistentné nasadzovanie potrebných softvérových opráv a aktualizácií
- implementácia nástrojov pre zavedenie viac-faktorovej autentifikácie
- implementácia nástrojov pre zavedenia manažmentu mobilných zariadení
- implementácia nástrojov, ktorých cieľom je zvýšiť schopnosť detekcie škodlivých aktivít a bezpečnostných incidentov, resp. ochrana koncových bodov, dát, dátových prenosov a sieťovej komunikácie, alebo ktorých cieľom je zvýšenie ochrany pred kybernetickými útokmi z externého prostredia

Projekt je formulovaný tak, aby po jeho realizácii nastal čo najväčší súlad zabezpečenia kybernetickej a informačnej bezpečnosti so zákonom o kybernetickej bezpečnosti, s vyhláškou 362/2018 Z. z. a so zákonom o ITVS.

Obmedzenia projektu:

Z hľadiska technického, personálneho, odborného, ale ani legislatívneho neevidujeme žiadne obmedzenia, ktoré by mohli ovplyvniť úspešnú realizáciu projektu.

3.3 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.	Administrátor IT	MŠVVaM SR	Zabezpečuje prevádzku IT systémov MŠVVaM SR	isvs_376, isvs_6092, isvs_6712, isvs_374, isvs_6301
2.	Manažér kybernetickej bezpečnosti	MŠVVaM SR	Zodpovedný za KIB MŠVVaM SR	isvs_376, isvs_6092, isvs_6712, isvs_374, isvs_6301
3.	Zamestnanec MŠVVaM SR	MŠVVaM SR	Využíva IS MŠVVaM SR	isvs_376, isvs_6092, isvs_6712, isvs_374, isvs_6301
4.	Občan / podnikateľ – používateľ ZS (verejnosť)		Využíva ZS poskytované MŠVVaM SR prostredníctvom jeho IS	isvs_376, isvs_6092, isvs_6712, isvs_374, isvs_6301
5.	Poskytovateľ IT služieb (verejnosť)		Poskytuje služby IS pre MŠVVaM SR	isvs_376, isvs_6092, isvs_6712, isvs_374, isvs_6301
6.	OVM		Poskytuje alebo konzumuje údaje IS MŠVVaM SR v podobe dátových zdrojov, otvorených dát alebo vo	isvs_376, isvs_6092, isvs_6712, isvs_374, isvs_6301

			forme služieb resp. rozhraní	

3.4 Ciele projektu

Ciele projektu sú definované v súlade s Národnou koncepciou informatizácie verejnej správy (ďalej len „NKIVS“) a súčasne sú definované tak, aby boli v súlade s očakávanými výsledkami definovanými v Partnerskej dohode Slovenskej republiky na roky 2021 – 2027 (ďalej len „Partnerská dohoda“) pre špecifický cieľ RSO 1.2. Definície cieľov rovnako vychádzajú z národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025.

Partnerská dohoda definuje špecifický cieľ RSO 1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy a konkrétne opatrenie: 1.2.1 Podpora v oblasti informatizácie a digitálnej transformácie, oblasť - Kybernetická a informačná bezpečnosť, pričom hlavným cieľom podpory je aj zabezpečenie kybernetickej bezpečnosti v súlade so Stratégiou digitálnej transformácie Slovenska. Stratégia digitálnej transformácie v oblasti kybernetickej bezpečnosti odkazuje na Národnú stratégiu kybernetickej bezpečnosti vydanú Národným bezpečnostným úradom (ďalej len „NBÚ“)

Národná koncepcia informatizácie verejnej správy určuje v rámci prioritnej osi 4 Kybernetická a informačná bezpečnosť strategickú prioritu Kybernetická a informačná bezpečnosť. Splnenie tejto strategickej priority má byť dosiahnuté nasledujúcimi dvoma cieľmi:

Cieľ 4.1 Zvýšenie schopnosti včasnej identifikácie kybernetických incidentov vo verejnej správe

Cieľ 4.2 Posilniť ľudské kapacity a vzdelávanie v oblasti kybernetickej a informačnej bezpečnosti patriace pod prioritnú os 4 Kybernetická a informačná bezpečnosť.

Z vyššie uvedených cieľov je pre projekt dôležitý cieľ 4.1 a v súlade s ním je aj nižšie citovaný strategický cieľ.

Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025, ktorá vychádza z Partnerskej dohody definuje vo vzťahu k verejnej správe nasledovný strategický cieľ:

4.1 Dôveryhodný štát pripravený na hrozby.

V definícii tohto strategického cieľa uvádza, cit:

„Kybernetická bezpečnosť je zodpovednosťou každého obyvateľa Slovenskej republiky, no bezpečnosť nemôže fungovať bez existencie mechanizmov na národnej úrovni, ktoré určujú politiku kybernetickej bezpečnosti, systém jej riadenia, ale aj procesy na detekciu a riešenie kybernetických bezpečnostných incidentov, budovanie odborných kapacít a šírenie situačného a bezpečnostného povedomia. Zároveň štát musí pri budovaní dôveryhodnosti vykonávať vyššie uvedené aktivity v súlade s Ústavou Slovenskej republiky a ostatnými zákonmi a vstupovať do základných ľudských práv a slobôd len v nevyhnutnej miere.“

Cieľový stav uvedeného strategického cieľa je v Národnej stratégii kybernetickej bezpečnosti na roky 2021 až 2025 stanovený nasledovne, cit.:

„Vybudovanie dostatočného odborného personálneho základu pre systém riadenia informačnej a kybernetickej bezpečnosti nielen na národnej, ale aj sektorovej úrovni. Spolupráca štátu s občanom na úrovni poskytovania dostatočných informácií a odporúčaní a realizácia krokov, ktoré občan reálne pocíti ako zvýšenie vlastnej bezpečnosti a bezpečnosti národného kybernetického priestoru. Vytvorenie a používanie certifikačných schém na široké portfólio typov výrobkov, procesov a služieb. Kvalitnejšie technické, organizačné a personálne zabezpečenie, založené na využívaní moderných prístupov ku kybernetickej bezpečnosti pri detekcii a riešení kybernetických bezpečnostných incidentov. Vybudovanie spôsobilostí na detekciu a riešenie kybernetických bezpečnostných incidentov na všetkých úrovniach. Efektívna spolupráca zainteresovaných subjektov na všetkých úrovniach riešenia informačnej a kybernetickej bezpečnosti. Dobre nastavený proces technickej, ale aj politickej atribúcie kybernetických bezpečnostných incidentov. Systematické a kontinuálne riadenie rizík kybernetickej bezpečnosti v jednotlivých sektoroch. Zlepšenie detekcie a zisťovania kybernetických bezpečnostných incidentov na sektorovej úrovni, zlepšenie a zjednodušenie nahlasovania kybernetických bezpečnostných incidentov nielen zo strany povinných subjektov, ale aj v rovine dobrovoľných hlásení. Podpora spôsobilostí subjektov v oblasti riadenia kontinuity činností.“

Všetky ciele projektu sú definované v súlade s vyššie uvedenými strategickými dokumentmi:

ID	Názov cieľa	Názov strategického cieľa*	Spôsob realizácie strategického cieľa
1	Zavedenie správy privilegovaných účtov Cieľ realizovaný v zmysle oprávnenej oblasti: Riadenie prístupov	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	- Dodanie softvérového vybavenia na správu privilegovaných účtov - Realizácia implementačných prác pri zavedení správy privilegovaných účtov
2.	Zavedenie aplikácie na správu a aktualizáciu bezpečnostnej dokumentácie	Dôveryhodný štát pripravený na hrozby	- Dodanie Aplikácie na správu a aktualizáciu bezpečnostnej dokumentácie

	Cieľ realizovaný v zmysle oprávnenej oblasti: Bezpečnosť pri prevádzke informačných systémov a sietí	(Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	- Realizácia implementačných prác pri zavedení Aplikácie na správu a aktualizáciu bezpečnostnej dokumentácie
3.	Zabezpečenie ochrany užívateľských zariadení pred kybernetickými hrozbami Cieľ realizovaný v zmysle oprávnenej oblasti: Ochrana proti škodlivému kódu	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	- Prechod na licencie ESET PROTECT Enterprise - Realizácia implementačných prác na zabezpečenie ochrany užívateľských zariadení pred kybernetickými útokmi
4.	Zabezpečenie ochrany serverov pred kybernetickými hrozbami Cieľ realizovaný v zmysle oprávnenej oblasti: Ochrana proti škodlivému kódu	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	- Dodanie nástroja na ochranu serverov pred kybernetickými hrozbami - Realizácia implementačných prác na zabezpečenie ochrany serverov pred kybernetickými hrozbami
5.	Zlepšenie sieťovej a komunikačnej bezpečnosti Cieľ realizovaný v zmysle oprávnenej oblasti: Sieťová a komunikačná bezpečnosť	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	- Dodávka Firewallov - Dodávka OOB firewallov - Dodávka nástroja na riadenie politík zabezpečenia sietí - Dodávka Web Application Firewall - Dodávka webových proxy - Realizácia implementačných prác spojených s vyššie uvedenými dodávkami za účelom zlepšenia sieťovej a komunikačnej bezpečnosti
6.	Rozšírenie logovacieho systému o korelácie a automatizáciu Cieľ realizovaný v zmysle o oprávnených oblastí: Zaznamenávanie udalostí a monitorovanie a Riešenie kybernetických bezpečnostných incidentov	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Rozšírenie licencií nástroja na zaznamenávanie udalostí a monitorovanie vybavenia na logovanie v rozsahu: - Splunk Enterprise - Splunk Enterprise Security - Splunk SOAR Realizácia implementačných prác za účelom rozšírenia logovacieho systému o korelácie a automatizáciu
7.	Implementácia podporných systémov pre zabezpečenie kontinuity prevádzky Cieľ realizovaný v zmysle oprávnenej oblasti: Kontinuita prevádzky	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	- Dodávka softvérového vybavenia pre implementáciu podporných systémov pre zabezpečenie kontinuity prevádzky - Realizácia implementačných prác pri zavedení podporných systémov pre zabezpečenie kontinuity prevádzky
8.	Zavedenie infraštruktúry pre prevádzku kybernetickej bezpečnosti a informačnej bezpečnosti Cieľ realizovaný v zmysle oprávnenej oblasti: Kontinuita prevádzky	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	- Dodávka serverov pre bezpečnostné opatrenia - Implementácia serverov pre bezpečnostné opatrenia
9.	Audity kybernetickej bezpečnosti Cieľ realizovaný v zmysle oprávnenej oblasti: Audity a kontrolné činnosti	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	- Realizácia pravidelného auditu kybernetickej bezpečnosti - Realizácia mimoriadneho auditu kybernetickej bezpečnosti

3.5 Merateľné ukazovatele (KPI)

ID	**ID/Názov cieľa**	**Názov ukazovateľa** (KPI)	**Popis ukazovateľa**	**Merná jednotka**	**AS IS merateľné hodnoty** (aktuálne)	**TO BE Merateľné hodnoty** (cieľové hodnoty)	**Spôsob ich merania**	**Pozn.**
1	PO095 / PSKPSOI12	Verejné inštitúcie podporované v rozvoji	Počet verejných inštitúcií, ktoré sú	verejné inštitúcie	0	1	Identifikácia počtu realizácie opatrení KIB pre inštitúciu –	Typ ukazovateľa: Výstup

		kybernetických služieb, produktov a procesov	podporované za účelom rozvoja a modernizácie kybernetických služieb, produktov, procesov a zvyšovania vedomostnej úrovne napríklad v kontexte opatrení smerujúcich k elektronickej bezpečnosti verejnej správy.				splnenie súladu KIB so zákonom o kybernetickej bezpečnosti a zákonom o ISVS Čas plnenia merateľného ukazovateľa projektu: Fyzické ukončenie realizácie hlavných aktivít projektu	
2	PR017 / PSKPRCR 11	Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov	Používateľ v oblasti KIB	používateli a / rok	0	700	Databáza používateľov v oblasti KIB. V prípade MŠVVaM SR ide o počet zamestnancov, ktorí využívajú IS MŠVVaM SR pri poskytovaní ZS. Čas plnenia merateľného ukazovateľa projektu: v rámci udržateľnosti projektu	Typ ukazovateľa: výsledok

3.5.1 Špecifikácia potrieb koncového používateľa

Z pohľadu MŠVVaM SR je koncovým používateľom IT oddelenie a sekundárne zamestnanci MŠVVaM SR, občania a podnikateľské subjekty, ktoré očakávajú, že nebude vplyvom kybernetických útokov dochádzať k výpadkom prevádzky IS mesta a tým sa de facto znefunkční poskytovanie ZS MŠVVaM SR.

Z výsledkov auditu kybernetickej bezpečnosti vyplynuli definície potrieb a požiadaviek na realizáciu opatrení KIB, v ktorých MŠVVaM SR ako PZS dosahuje najvyšší nesúlad v zmysle zákona o kybernetickej bezpečnosti, zákona o ISVS a vyhlášky 362/2018 Z. z. Ide o :

- Potrebu zlepšenia riadenia prístupov – realizáciu opatrenia pre **správu privilegovaných účtov**
- Potrebu zvýšenia bezpečnosti pri prevádzke informačných systémov a sietí – **zavedením aplikácie na správu a aktualizáciu bezpečnostnej dokumentácie**
- Zvýšenie ochrany proti škodlivému kódu – **zavedením ochrany užívateľských zariadení pred kybernetickými hrozbami**
- Zvýšenie ochrany proti škodlivému kódu – **zavedením ochrany serverov pred kybernetickými hrozbami**
- Potrebu zvýšenia sieťovej a komunikačnej bezpečnosti – **zlepšením sieťovej a komunikačnej bezpečnosti**
- Zvýšenie úrovne zaznamenávania udalostí a monitorovania, ako aj riešenia kybernetických bezpečnostných incidentov – **rozšírením nástroja na zaznamenávanie udalostí a monitorovanie**
- Zavedenie infraštruktúry pre prevádzku kybernetickej bezpečnosti
- Realizáciu auditov a kontrolných činností – **vykonaním auditu v roku 2025 (pravidelný audit KIB) a mimoriadneho auditu po ukončení implementácie opatrení KIB**.

Podrobne boli špecifikované požiadavky na realizáciu v rámci prieskumov trhu na realizáciu opatrení nasledovne:

Zákazka č. 1: Zvýšenie úrovne kybernetickej a informačnej bezpečnosti Ministerstva školstva, výskumu, vývoja a mládeže Slovenskej republiky

Realizáciou predmetu zákazky verejný obstarávateľ realizuje nasledovné oprávnené oblasti v zmysle výzvy Zvýšenie úrovne kybernetickej a informačnej bezpečnosti, číslo výzvy: PSK-MIRRI-616-2024-DV-EFRR (ďalej len „výzva“)

- Riadenie prístupov
- Bezpečnosť pri prevádzke informačných systémov a sietí

- Ochrana proti škodlivému kódu
- Sieťová a komunikačná bezpečnosť
- Zaznamenávanie udalostí a monitorovanie
- Riešenie kybernetických bezpečnostných incidentov
- Kontinuita prevádzky

Realizáciou tejto zákazky verejný obstarávateľ sleduje splnenie nasledovných cieľov, ktoré zároveň reprezentujú predmet obstarania:

1. Zavedenie správy privilegovaných účtov
2. Zavedenie aplikácie na správu a aktualizáciu bezpečnostnej dokumentácie
3. Zabezpečenie ochrany užívateľských zariadení pred kybernetickými hrozbami
4. Zabezpečenie ochrany serverov pred kybernetickými hrozbami
5. Zlepšenie sieťovej a komunikačnej bezpečnosti
6. Rozšírenie logovacieho systému o korelácie a automatizáciu
7. Implementácia podporných systémov pre zabezpečenie kontinuity prevádzky
8. Zavedenie infraštruktúry pre prevádzku kybernetickej bezpečnosti a informačnej bezpečnosti

1. Zavedenie správy privilegovaných účtov

Cieľom verejného obstarávateľa je obstaranie a nasadenie systému pre správu a administráciu privilegovaných účtov (ďalej len "PIM/PAM"), ktorý zabezpečí jednotnú správu prístupov k privilegovaným účtom a monitorovanie operácií vykonávaných pod týmito účtami s prepojením na konkrétneho administrátora, ktorý účet aktuálne používa, vrátane dvojfaktorovej autentifikácie a zabezpečenie detailného oboznámenia sa so správou dodaného systému pre IT pracovníkov verejného obstarávateľa.

Predmetom dodávku bude Nástroj na správu privilegovaných účtov.

V rámci dodávky budú realizované nasledovné činnosti:

- Vypracovanie Detailného návrhu riešenia
- Implementácia technického riešenia v rámci technickej špecifikácie:
- Testovanie a overovanie funkčnosti riešenia:
- Nasadenie

2. Zavedenie aplikácie na správu a aktualizáciu bezpečnostnej dokumentácie

Požaduje sa dodanie a inštalácia *Aplikácie na správu a aktualizáciu bezpečnostnej dokumentácie* do virtuálneho servera spravovaného verejným obstarávateľom.

3. Zabezpečenie ochrany užívateľských zariadení pred kybernetickými hrozbami

Na koncových staniciach užívateľov je implementovaná základná ochrana proti škodlivému kódu na platforme ESET PROTECT, vo verzii ADVANCED.

Verejný obstarávateľ plánuje v tomto projekte zvýšiť súčasnú ochranu užívateľských zariadení proti škodlivému kódu implementáciou nasledovných nástrojov:

- platformy na proaktívnu detekciu hrozieb, efektívnu identifikáciu neobvyklého správania v sieti a včasnú nápravu s cieľom predchádzať únikom dát a narušeniu firemnej prevádzky
- nástroj umožňujúci XDR, poskytujúci riadenie rizík a prehľad o hrozbách a systéme, ktorý umožňuje vykonávať rýchlu a hĺbkovú analýzu príčin vzniku incidentov a okamžite na ne reagovať.

Uvedené funkcionality vylepšenej ochrany pred škodlivým kódom budú dosiahnuté prechodom na licencie ESET PROTECT Enterprise

V rámci dodávky budú realizované nasledovné činnosti:

- Vypracovanie Detailného návrhu riešenia
- Inštalácia
- Implementácia a testovanie
- Nasadenie

4. Zabezpečenie ochrany serverov pred kybernetickými hrozbami

Verejný obstarávateľ požaduje, aby uchádzač rozšíril súčasné riešenie o Enterprise Detection and Response (EDR) funkcionalitu.

V rámci dodávky budú realizované nasledovné činnosti:

- Vypracovanie Detailného návrhu riešenia
- Implementácia a testovanie

- Nasadenie

5. Zlepšenie sieťovej a komunikačnej bezpečnosti

Obnova perimetra firewallov – predmetom obnovy perimetra firewallow bude dodávka **dvoch** zariadení, **ktoré budú pracovať v HA zapojení.** V rámci dodávky budú realizované nasledovné činnosti:

- Vypracovanie Detailného návrhu riešenia
- Inštalácia zariadení
- Implementácia a testovanie
- Nasadenie

Obnova OOB firewallov – predmetom obnovy OOB bude dodávka 2 OOB. V rámci dodávky budú realizované nasledovné činnosti:

- Vypracovanie Detailného návrhu riešenia
- Inštalácia zariadení

Nástroj na riadenie politík zabezpečenia sietí – predmetom dodávky bude softvérový nástroj na riadenie politík zabezpečenia sietí. V rámci dodávky budú realizované nasledovné činnosti:

- Vypracovanie Detailného návrhu riešenia
- Inštalácia zariadení
- Implementácia a testovanie
- Nasadenie

Obnova WAF zariadení – predmetom dodávky bude obnova existujúcich WAF zariadení podľa požiadaviek zadávateľa (2 ks F5 BIG-IP i2800 alebo ekvivalentné zariadenie). V rámci dodávky budú realizované nasledovné činnosti:

- Vypracovanie Detailného návrhu riešenia
- Inštalácia zariadení
- Implementácia a testovanie
- Nasadenie

Nasadenie webových proxy – predmetom dodávky bude softvérový nástroj na realizáciu webových proxy. V rámci dodávky budú realizované nasledovné činnosti:

- Vypracovanie Detailného návrhu riešenia
- Inštalácia zariadení
- Implementácia a testovanie
- Nasadenie

6. <u>Rozšírenie logovacieho systému o korelácie a automatizáciu</u>

Verejný obstarávateľ disponuje licenciou Splunk Enterprise s výkonom 100GB/deň, platnou do 8.7.2026. Požaduje sa dodať licenčné rozšírenie existujúceho softvérového vybavenia minimálne o nasledovné komponenty (alebo ich ekvivalenty plne kompatibilné s existujúcimi licenciami): Splunk Enterprise (1 ks), Splunk Enterprise Security (1 ks), Splunk SOAR (2 ks). V rámci dodávky budú realizované nasledovné činnosti:

- Vypracovanie Detailného návrhu riešenia pre moduly SIEM a SOAR
- Implementácia a testovanie:
- Nasadenie

7. <u>Implementácia podporných systémov pre zabezpečenie kontinuity prevádzky</u>

Verejný obstarávateľ požaduje dodávku nasledovných licencií, pričom definované požiadavky sú stanovené ako minimálne:

ID	Názov položky	Licencie pre podporné systémy pre zabezpečenie kontinuity prevádzky
1a.	Názov licencie	Microsoft Windows Server Standard Edition 16 cores
1b.	Počet kusov	4
1c.	Servisná podpora	Bez servisnej podpory
1a.	Názov licencie	Microsoft SQL Server Enterprise Edition 2 cores
1b.	Počet kusov	6
1c.	Servisná podpora	Bez servisnej podpory

V rámci dodávky budú realizované nasledovné činnosti:

- Vypracovanie Detailného návrhu riešenia infraštruktúry v záložnej lokalite a obnovy záloh na ňu
- Implementácia a testovanie
- Nasadenie

8. Zavedenie infraštruktúry pre prevádzku kybernetickej bezpečnosti a informačnej bezpečnosti

Verejný obstarávateľ požaduje dodať infraštruktúru pre prevádzku bezpečnostných nástrojov a uchovávaných dát v nich, ktorá sa skladá z troch virtualizačných serverov. Tieto servre budú fyzicky oddelené od ostatnej infraštruktúry avšak budú zdieľať sieťovú, zálohovaciu a monitorovaciu infraštruktúru. V rámci dodávky budú realizované nasledovné činnosti:

- Vypracovanie Detailného návrhu riešenia
- Implementácia a testovanie
- Nasadenie

Zákazka č. 2: Audit kybernetickej bezpečnosti

Predmetom zákazky je poskytnúť verejnému obstarávateľovi cenovú ponuku pre vykonanie auditu kybernetickej bezpečnosti v prostredí *Ministerstva školstva, vedy, výskumu a športu Slovenskej republiky*, ktorý musí byť realizovaný podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov v súlade s vyhláškou NBÚ č. 493/2022 Z. z. o audite kybernetickej bezpečnosti, vyhláškou NBÚ č. 492/2022 o znalostných štandardoch a s vyhláškou NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení prevádzkovateľa základnej služby vo verzií účinnosti od 1. septembra 2023 (vyhláška č. 264/2023 Z. z.).

Požiadavky na predmet zákazky:

Názov	**Upresnenie**
Identifikácia základných služieb podporených auditovanými informačnými systémami a sieťami:	- Centrálna elektronická prihláška na vysoké školy (CEP) - Rezortný informačný systém (RIS) - Centrálny register zamestnancov VŠ (CRZ) - Centrálny register študentov vysokých škôl (CRS) - Portál Ministerstva školstva, vedy, výskumu a športu SR (PMS) - Portál elektronických služieb regionálneho a vysokého školstva (ESVRŠ) - Sofia
Počet zamestnancov prevádzkovateľa základnej služby:	722 interných zamestnancov 216 zamestnancov na dohodu o vykonaní práce alebo dohody o pracovnej činnosti
Počet informačných systémov s väzbou na základné služby:	17
Počet pracovníkov zúčastňujúcich na prevádzke IS:	111
Počet lokalít:	2
Počet tretích strán zúčastňujúcich na prevádzke IS:	6
Verejný obstarávateľ je zapojený do siete Govnet:	Áno
Verejný obstarávateľ nevlastní platný certifikát ISMS:	Nie
Odhadovaný počet externých zaregistrovaných používateľov základných služieb:	CEP: 4233 RIS: pristupuje 6900 škôl/zriaďovateľov CRZ: 64 CRS: 384 PMS: Návštevy 10,8 mil./ročne

	ESVRŠ: nevyžaduje sa registrácia, prihlasuje sa prostredníctvom OP (slovensko.sk) Sofia: 14000
Zaregistrovaný informačný systém najvyššej kategórie:	II. kategória
Nevyskytol sa u objednávateľa za posledné 2 roky závažný kybernetický bezpečnostný incident:	Nie
U objednávateľa nebol vykonaný audit kybernetickej bezpečnosti ani nebola uložená pokuta za porušenie povinnosti podľa zákona č. 69/2018 Z. z.:	Auditná správa kybernetickej bezpečnosti z dňa 13.12.2023

Fázaauditu	**Termín**
Nastavenie a výkon auditu kybernetickej bezpečnosti	Október 2025
Záverečná správa o výsledkoch auditu kybernetickej bezpečnosti (Správa)	Do 13.12.2025
Nastavenie a výkon **mimoriadneho** auditu kyber.ckej bezpečnosti	Október 2027
Záverečná správa o výsledkoch **mimoriadneho** auditu kybernetickej bezpečnosti (Správa)	Do 15.11.2027

.

3.6 Riziká a závislosti

Zoznam rizík a závislostí je detailne rozpracovaný v prílohe tohto dokumentu č. 1: Zoznam rizík a závislostí. Tento zoznam bude počas celej realizácie projektu aktualizovaný.

3.7 Stanovenie alternatív v biznisovej vrstve architektúry

Posudzovanie alternatív riešenia vychádza z viacerých možností. V prípade MŠVVaM SR, ktoré má zabezpečenú strednú úroveň kybernetickej bezpečnosti prichádzajú do úvahy nasledovné alternatívy:

0. Ponechanie existujúceho stavu – ide o nultý stav, v ktorom na základe auditu KIB boli identifikované nesúlady s legislatívnymi požiadavkami a možné ohrozenie ISVS a teda aj základných služieb MŠVVaM SR kybernetickým útokom.
1. Realizácia projektu KIB s riešením vybraných opatrení (t.j. nie všetkých nevyhnutných), ktoré identifikoval audit KIB ako tie, v ktorých je kritický nesúlad so zákonom o kybernetickej bezpečnosti a vyhláškou č. 362/2018 Z. z.– t.j. došlo by k zvýšeniu súladu s legislatívou, ale informačné systémy mesta by boli naďalej kriticky ohrozené.
2. Realizácia všetkých potrebných opatrení na dosiahnutie zvýšenia súladu KIB s požiadavkami zákona o kybernetickej bezpečnosti a zákona o ISVS – pôjde o také zvýšenie súladu s požiadavkami príslušnej legislatívy v oblasti KIB, ktorá zabezpečí ochranu IS MŠVVaM SR pred čo najväčším objemom hrozieb, pričom niektoré opatrenia KIB budú realizované formou služby.
3. Realizácia opatrení na dosiahnutie zvýšenia súladu KIB s požiadavkami zákona o kybernetickej bezpečnosti a zákona o ISVS – pôjde o také zvýšenie súladu s požiadavkami príslušnej legislatívy v oblasti KIB, ktorá zabezpečí ochranu IS MŠVVaM SR pred najväčšími hrozbami, pričom by šlo o in house riešenie s prevádzkou na úrovni MŠVVaM SR.

Z hľadiska identifikovaných procesov v kapitole 3.2.2 alternatíva 0 nepokryje riešenie žiadneho z identifikovaného problémov. V prípade čiastkového riešenia (alternatíva 1) by boli zvolené iba niektoré z procesov, ktoré by boli projektom vyriešené. V prípade alternatívy 2 budú podporené všetky procesy v oblasti KIB, ktoré je potrebné pre účely ochrany IS, a ktoré zabezpečujú prevádzku základnej služby MŠVVaM SR, riešiť – avšak niektoré opatrenia budú musieť byť realizované dodávateľsky. Z hľadiska závažnosti kybernetickej bezpečnosti, finančnej udržateľnosti zo strany MŠVVaM a nakoľko disponuje expertným tímom sa realizuje ako finančne najvýhodnejšie a súčasne garantujúce úspešnosť projektu zvolenie alternatívy 3 – kompletné in-house riešenie.

3.8 Multikriteriálna analýza

Multikriteriálna analýza je v tomto prípade redukovaná na dva parametre:

1. Potrebu zosúladenia úrovne kybernetickej bezpečnosti s požiadavkami zákona o kybernetickej bezpečnosti a zákona o ITVS. Táto požiadavka sa dotýka všetkých stakeholderov a predstavuje KO kritérium. Ak nemá dôjsť k zásadnému zvýšeniu kybernetickej a informačnej bezpečnosti, t.j. ak má zostať ponechaný stav alebo iba dôjde k čiastočnému zlepšeniu, nebude možné považovať realizovaný projekt za úspešný.
2. Udržateľnosť riešenia.

Z vyššie uvedených možných alternatív(viď kapitola 3.7) vyplýva, že s ohľadom na potreby a finančné možnosti MŠVVaM SR je najvýhodnejšia a dlhodobo udržateľná alternatíva 3.

3.9 Stanovenie alternatív v aplikačnej vrstve architektúry

HW a SW komponenty, rovnako ako služby, ktoré sú s nimi spojené musia zodpovedať požiadavkám definovaným v projekte koncovými používateľmi - tými sú v tomto prípade oddelenie informatiky, ktoré vychádza z požiadaviek zákona o kybernetickej bezpečnosti, zákona o ITVS, vyhlášky 362/2018 Z. z. a ďalších predpisov.

Aplikačná vrstva predpokladá dve alternatívy:

I. realizácia všetkých opatrení na úrovni MŠVVaM SR v zmysle definovaných požiadaviek, pričom všetky technológie na realizáciu opatrení KIB budú vytvorené ako IN-HOUSE riešenie- táto architektúra zodpovedá alternatíve 3 popísanej v multikriteriálnej analýze

II. realizácia všetkých opatrení na úrovni MŠVVaM SR v zmysle definovaných požiadaviek, pričom niektoré technológie na realizáciu opatrení KIB budú vytvorené ako IN-HOUSE riešenie a niektoré ako služba - táto architektúra zodpovedá alternatíve 2 popísanej v multikriteriálnej analýze.

S ohľadom na reálne potreby a požiadavky MŠVVaM SR, zohľadňujúc materiálne a personálne kapacity bude aplikačne zvolená alternatíva I.

3.10 Stanovenie alternatív v technologickej vrstve architektúry

Z hľadiska použitých technológií nie sú definované alternatívy. Požiadavky na technológie sú definované všeobecne tak, aby ľubovoľnú SW a HW technológia, ktorá splní definované požiadavky bolo možné použiť na realizáciu projektu.

Technologickú architektúru riešenia definuje nasledovný obrázok:

4. POŽADOVANÉ VÝSTUPY (PRODUKT PROJEKTU)

Výsledkom projektu budú:

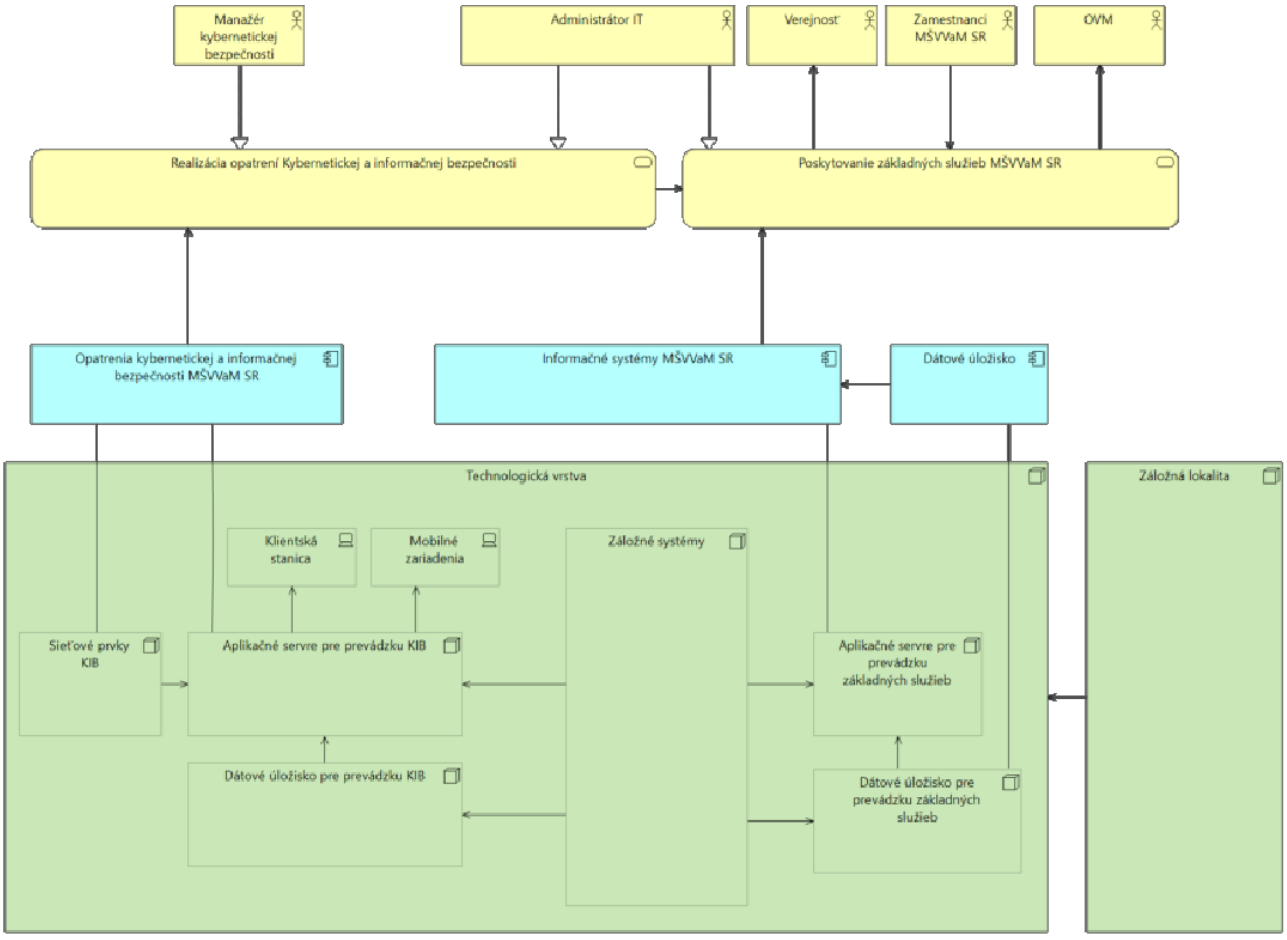
- Projektové výstupy v zmysle vyhlášky 401/2023 o riadení projektov. V prípade, že predmetom realizácie bude dielo (oceniteľné práva a/alebo zdrojový kód), získa MŠVVaM SR právo vykonávať autorské práva k tomuto dielu, vrátane výhradnej a územne neobmedzenej licencie. Tieto podmienky sa nevzťahujú na tzv. krabicový softvér, ktorý je predávaný ako produkt či už realizátora alebo tretej strany.
- Z hľadiska plnenia cieľov projektu bude výsledkom projektu naplnenie hlavného cieľa, t.j. najvyšší možný súlad KIB so zákonom o kybernetickej bezpečnosti a so zákonom o ITVS, čo bude naplnené realizáciu nasledovných partikulárnych cieľov:
    - Zavedenie správy privilegovaných účtov
    - Zavedenie aplikácie na správu a aktualizáciu bezpečnostnej dokumentácie
    - Zabezpečenie ochrany užívateľských zariadení pred kybernetickými hrozbami
    - Zabezpečenie ochrany serverov pred kybernetickými hrozbami
    - Zlepšenie sieťovej a komunikačnej bezpečnosti
    - Rozšírenie logovacieho systému o korelácie a automatizáciu
    - Implementácia podporných systémov pre zabezpečenie kontinuity prevádzky
    - Zavedenie infraštruktúry pre prevádzku kybernetickej bezpečnosti a informačnej bezpečnosti
    - Audity kybernetickej bezpečnosti

- Technologicky a administratívne pôjde o realizáciu nasledovných cieľov:
    - Dodanie softvérového vybavenia na správu privilegovaných účtov
    - Realizácia implementačných prác pri zavedení správy privilegovaných účtov
    - Dodanie Aplikácie na správu a aktualizáciu bezpečnostnej dokumentácie
    - Realizácia implementačných prác pri zavedení Aplikácie na správu a aktualizáciu bezpečnostnej dokumentácie
    - Prechod na licencie ESET PROTECT Enterprise
    - Realizácia implementačných prác na zabezpečenie ochrany užívateľských zariadení pred kybernetickými útokmi

- Dodanie nástroja na ochranu serverov pred kybernetickými hrozbami
- Realizácia implementačných prác na zabezpečenie ochrany serverov pred kybernetickými hrozbami
- Dodávka Firewallov
- Dodávka OOB firewallov
- Dodávka nástroja na riadenie politík zabezpečenia sietí
- Dodávka Web Application Firewall
- Dodávka webových proxy
- Realizácia implementačných prác spojených s vyššie uvedenými dodávkami za účelom zlepšenia sieťovej a komunikačnej bezpečnosti
- Rozšírenie licencií nástroja na zaznamenávanie udalostí a monitorovanie vybavenia na logovanie v rozsahu:
  - Splunk Enterprise
  - Splunk Enterprise Security
  - Splunk SOAR
- Realizácia implementačných prác za účelom rozšírenia logovacieho systému o korelácie a automatizáciu
- Dodávka softvérového vybavenia pre implementáciu podporných systémov pre zabezpečenie kontinuity prevádzky
- Realizácia implementačných prác pri zavedení podporných systémov pre zabezpečenie kontinuity prevádzky
- Dodávka serverov pre bezpečnostné opatrenia
- Implementácia serverov pre bezpečnostné opatrenia
- Realizácia pravidelného auditu kybernetickej bezpečnosti
- Realizácia mimoriadneho auditu kybernetickej bezpečnosti

5. NÁHĽAD ARCHITEKTÚRY

Architektúra celého riešenia je rámcová tak, aby bolo z projektu zrejmé, ktoré komponenty v rámci realizácie projektu budú vytvorené, rozšírené alebo upravené (a budú realizovať opatrenia KIB).
Primárne opatrenia kybernetickej bezpečnosti chránia IS MŠVVaM SR, ktoré sú určené na prevádzkovanie základných služieb MŠVVaM SR.



Obrázok: Celková architektúra riešenia

6. LEGISLATÍVA

V rámci platnej legislatívy nebude potrebné meniť žiadnu legislatívu. Projekt je realizovaný za účelom dosiahnutia súladu s platnou legislatívou a to najmä:

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 č.78/2020 Z.z. o štandardoch pre ITVS

Vyhláška č.401/2023 Z.z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy

Vyhláška 179/2020 Z.z. o obsahu bezpečnostných opatrení ITVS

Vyhláška 362/2018 Z.z. o obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení)

7. ROZPOČET A PRÍNOSY

V uvedenom projekte vychádzame pri stanovení rozpočtu z prieskumu trhu a pravidiel stanovených výzvou. S ohľadom na rozpočet projektu (projekt nad 1 000 000,00,- EUR) bola spracovaná Analýza nákladov a prínosov, ktorá je prílohou tohto projektového zámeru.

V prípade projektov kybernetickej bezpečnosti je priame vyčíslenie návratnosti pomerne komplikované. Z pohľadu návratnosti je potrebné venovať sa hodnoteniu možných škôd, ktoré by potenciálne vznikli v prípade, že nebude adekvátne riešená KIB na úrovni poskytovateľa základnej služby. Nakoľko tieto škody nie je možné kvantifikovať v plnom rozsahu objektívnymi parametrami, pri hodnotení finančných prínosov sme vychádzali iba z kvantifikovateľných prínosov, t.j. z monetizovateľných odhadov škôd, ktoré by spôsobil jeden závažný incident KIB.

V prípade realizácie projektu berieme do úvahy nasledovné potenciálne škody:

Finančné riziko – vyhodnotenie straty interných finančných prostriedkov. V prípade, že nebudú adekvátne implementované opatrenia KIB bolo hodnotenie možného výpadku základnej služby definované na 10 pracovných dní.

V prípade 722 TPP zamestnancov MŠVVaM SR ide o 54150,00 hodín. Priemerná mesačná mzda v roku 2023 vo verejnej správe bola 1796 EUR, t.j. priemerná cena za jednu hodinu práce bola 11,63 EUR. Celková strata v prípade výpadku základnej služby na úrovni straty miezd TPP zamestnancov MŠVVaM SR by predstavovala 629764,50 EUR v prípade jedného výpadku na základe kybernetického útoku.

V prípade 216 zamestnancov na dohodu MŠVVaM SR ide o 4320,00 hodín. Priemerná mesačná mzda v roku 2023 vo verejnej správe bola 1796 EUR, t.j. priemerná cena za jednu hodinu práce bola 11,63 EUR (viď údaje Štatistického úradu Slovenskej republiky za rok 2023). Celková strata v prípade výpadku základnej služby na úrovni straty miezd zamestnancov na dohodu MŠVVaM SR by predstavovala 50241,60 EUR v prípade jedného výpadku na základe kybernetického útoku.

Celková strata interných finančných prostriedkov v prípade jedného KIB incidentu by teda bola: 680006,10 EUR

Finančné riziko – vyhodnotenie straty externých finančných prostriedkov. V prípade, že nebudú adekvátne implementované opatrenia KIB bolo hodnotenie možného výpadku základnej služby definované na 10 pracovných dní. V prípade externých používateľov ZS pôjde o celkový výpadok 154805,00 používateľských hodín. Priemerná mesačná mzda v roku 2023 v národnom hospodárstve bola 1430 EUR, t.j. priemerná cena za jednu hodinu práce bola 8,25 EUR (viď údaje Štatistického úradu Slovenskej republiky za rok 2023).

Celková strata externých finančných prostriedkov v prípade jedného KIB incidentu by teda bola 1277141,25 EUR.

Finančné riziko – dôsledky kybernetického útoku. Ide o možné sankcie vyplývajúce priamo z legislatívnych rámcov, prípadných súdnych sporov (v prípade napríklad úniku osobných údajov), ako aj nákladov spojených so sanáciou prípadného kybernetického incidentu. Tieto finančné prostriedky nie je možné momentálne vyčísliť, reálne však môže niekoľko násobne prekročiť straty interných finančných prostriedkov MŠVVaM SR.

Reputačné riziko – vzhľadom na postavenie a oblasť spoločenskej dôležitosti a zákonných povinností MŠVVaM SR, je toto riziko potenciálne vysoké – teda v prípade neplnenia legislatívnych požiadaviek v zmysle zákona o kybernetickej bezpečnosti a zákona o ITVS, reálneho výpadku prevádzky základnej služby, úniku citlivých dát v kombinácii aj s prípadnou medializáciou a pod.

7.1 Sumarizácia nákladov a prínosov

Finančná analýza projektu a rozpočet bude predmetom inciačnej fázy projektu.

8. HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU A METÓDA JEHO RIADENIA

ID	FÁZA/AKTIVITA	ZAČIATOK (odhad termínu)	KONIEC (odhad termínu)	POZNÁMKA
1.	Prípravná fáza a Iniciačná fáza	08/2024	10/2025	Začiatok realizačnej fázy projektu vyplýva z predpokladu, že realizácia projektu začne až po ukončení administratívneho a odborného hodnotenia a po podpise Zmluvy o poskytnutí NFP, pričom je definovaná dostatočná časová rezerva na tieto úkony. Rovnako na procesy verejného obstarávania, ktoré môžu potenciálne začať v krátkom čase po podaní žiadosti o NFP.
2.	Realizačná fáza	11/2025	10/2027	
2a	Analýza a Dizajn	11/2025	06/2026	
2b	Nákup technických prostriedkov, programových prostriedkov a služieb	11/2025	03/2026	
2c	Implementácia a testovanie	04/2026	05/2027	
2d	Nasadenie a PIP	06/2027	10/2027	
3.	Podpora prevádzky (SLA)	11/2027	10/2032	Po ukončení projektu začína fáza udržateľnosti projektu, t.z. podpora prevádzky (SLA). V rámci danej fázy bude prijímateľ udržiavať a využívať implementované systémy. Vzniknuté náklady v tejto fáze projektu bude hradiť z vlastných výdavkov, na čo v rozpočte každoročne vyčlení dostatok finančných prostriedkov.

Projekt bude realizovaný metódou Waterfall s logickými nadväznosťami realizácie jednotlivých modulov na základe funkčnej a technickej špecifikácie vypracovanej v rámci prípravy projektu.

Tento prístup bol zvolený nakoľko opatrenia KIB je potrebné realizovať vo vzájomných súvislostiach, avšak v správnom postupe. Niektoré môžu byť realizované paralelne, dokonca rôznymi tímami, avšak na základe vopred stanovenej stratégie a plánu celého projektu. Agilný prístup na realizáciu nami plánovaného projektu nie je vhodný i s ohľadom na potrebu realizácie projektu za plnej prevádzky základnej služby MŠVVaM SR.

9. PROJEKTOVÝ TÍM

Zostavuje sa Riadiaci výbor (RV), v minimálnom zložení:

- Predseda RV – PhDr. Mgr. Ľubomír Nebeský, PhD., GR kancelárie GTSÚ
- Biznis vlastník – Ing. Martin Horňák, riaditeľ odboru správy informačných systémov
- Zástupca prevádzky – Bc. Štefan Jenčuš, poverený riaditeľ odboru podporných IT služieb
- Projektový manažér objednávateľa (PM) – JUDr. Ing. Jana Barjaková, riaditeľka organizačného odboru generálneho tajomníka služobného úradu

Zostavuje sa Projektový tím objednávateľa:

- Kľúčový používateľ - PhDr. Mgr. Ľubomír Nebeský, PhD., GR kancelárie GTSÚ
- IT architekt – Martin Bokor
- IT analytik – Mgr. Miroslav Odor, MKIB
- Biznis vlastník – Ing. Martin Horňák, riaditeľ odboru správy informačných systémov
- Manažér kvality – JUDr. Jozef Stopka
- Manažér kybernetickej a informačnej bezpečnosti – Mgr. Miroslav Odor, MKIB
- Projektový manažér (pre účely realizácie) – JUDr. Ing. Jana Barjaková, riaditeľka organizačného odboru generálneho tajomníka služobného úradu (s využitím ext. služieb hradených z paušálnych výdavkov)

ID	Meno a Priezvisko	Pozícia	Oddelenie	Rola v projekte

1.	PhDr. Mgr. Ľubomír Nebeský, PhD	GR kancelárie GTSÚ	MŠVVaM SR	Kľúčový používateľ
	Martin Bokor	IT špecialista - architekt pre SHMÚ	SHMÚ IT oddelenie	IT architekt
2.	Mgr. Miroslav Odor	IT analytik	MŠVVaM SR	IT analytik
3.	Ing. Martin Horňák	riaditeľ odboru správy informačných systémov	MŠVVaM SR	Biznis vlastník
4.	JUDr. Jozef Stopka	špecialista riadenia systému manažérstva kvality modelu CAF	MŠVVaM SR	Manažér kvality
5.	Mgr. Miroslav Odor	MKIB	MŠVVaM SR	Manažér kybernetickej a informačnej bezpečnosti
6.	JUDr. Ing. Jana Barjaková	riaditeľka organizačného odboru generálneho tajomníka služobného úradu (s využitím ext. služieb hradených z paušálnych výdavkov)	MŠVVaM SR	Projektový manažér (pre účely realizácie)

Uvedený projektový tím je garanciou úspešnej realizácie projektu po zabezpečení jeho financovania na základe ŽoNFP v rámci výzvy. Všetci členovia projektového tímu budú pred začiatkom projektu zamestnancami MŠVVaM SR. Niektorí sú zamestnancami v súčasnosti, ďalší sa zaviazali nastúpiť do pracovného pomeru k termínu začatia projektu.

9.1 PRACOVNÉ NÁPLNE

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

Projektová rola:	**IT ARCHITEKT**
Stručný popis:	• zodpovedá za návrh architektúry riešenia IS a implementáciu technológií predovšetkým z pohľadu udržateľnosti, kvality a nákladov, za riešenie architektonických cieľov projektu dizajnu IS a súlad s architektonickými princípmi. • vykonáva, prípadne riadi vysoko odborné tvorivé činnosti v oblasti návrhu IT. Študuje a stanovuje smery technického rozvoja informačných technológií, navrhuje riešenia na optimalizáciu a zvýšenie efektívnosti prostriedkov výpočtovej techniky. Navrhuje základnú architektúru informačných systémov, ich komponentov a vzájomných väzieb. Zabezpečuje projektovanie dizajnu, architektúry IT štruktúry, špecifikácie jej prvkov a parametrov, vhodnej softvérovej a hardvérovej infraštruktúry podľa základnej špecifikácie riešenia. • zodpovedá za spracovanie a správu projektovej dokumentácie a za kontrolu súladu implementácie s dokumentáciou. Môže tiež poskytovať konzultácie, poradenstvo a vzdelávanie v oblasti svojej špecializácie. IT architekt, projektant analyzuje, vytvára a konzultuje so zákazníkom riešenia na úrovni komplexných IT systémov a IT architektúr, najmä na úrovni aplikačného vybavenia, infraštruktúrnych systémov, sietí a pod. Zaručuje, že návrh architektúry a/alebo riešenia zodpovedá zmluvne dohodnutým požiadavkám zákazníka v zmysle rozsahu, kvality a ceny celej služby/riešenia.
Detailný popis rozsahu zodpovednosti, povinností a kompetencií	Zodpovedný za: • Navrhovanie architektúry IT riešení s cieľom dosiahnuť najlepšiu efektivitu. • Transformovanie cieľov, prísľubov a zámerov projektu do tvorby reálnych návrhov a riešení. • Navrhovanie takých riešení, aby poskytovali čo najvyššiu funkčnosť a flexibilitu. • Posudzovanie vhodnosti navrhnutých riešení s ohľadom na požiadavky projektu. • Zodpovednosť za technické navrhnutie a realizáciu projektu. • Zodpovednosť za vytvorenie technickej IT dokumentácie a jej následná kontrola. • Zodpovednosť za definovanie integračných vzorov, menných konvencií, spôsobov návrhu a spôsobu programovania. • Definovanie architektúry systému, technických požiadaviek a funkčného modelu (Proof Of Concept.) • Vytvorenie požiadaviek na HW/SW infraštruktúru IS

	• Udržiavanie a rozvoj konzistentnej architektúry s dôrazom na architektúru aplikačnú, dátovú a infraštruktúru • Analýzu a odhad náročnosti technických požiadaviek na vytvorenie IS alebo vykonanie zmien v IS • Navrhovanie riešení zohľadňujúce architektonické štandardy, časové a zdrojové obmedzenia, • Navrhovanie dátových transformácií medzi dátovými skladmi a aplikáciami • Vyhodnocovanie implementačných alternatív z pohľadu celkovej IT architektúry • Ladenie dátových štruktúr za účelom dosiahnutia optimálneho výkonu • Prípravu akceptačných kritérií • Analýza nových nástrojov, produktov a technológií • Správa, rozvoj a dohľad nad dodržiavaním integračných štandardov • Priebežné posudzovanie vecných výstupov dodávateľa v rámci analýzy, návrhu riešenia vrátane Detailného návrhu riešenia (DNR) z pohľadu analýzy a návrhu riešenia architektúry IS • Vykonáva posudzovanie a úpravu testovacej stratégie, testovacích scenárov, plánov testov, samotné testovanie a účasť na viacerých druhoch testovania • Vykonanie záťažových, výkonnostných a integračných testov a navrhnutie následných nápravných • Nasadenie a otestovanie migrácie, overenie kvality dát a navrhnutie nápravných opatrení • Participáciu na výkone bezpečnostných testov, • Participáciu na výkone UAT testov, • Posúdenie prevádzkovo-infraštruktúrnej dokumentácie pred akceptáciou a prevzatím od dodávateľa • Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 85/2020 Z.z., Prílohou č.1 • Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

Projektová rola:	**IT ANALYTIK**
Stručný popis:	• zodpovedá za zber a analyzovanie funkčných požiadaviek, analyzovanie a spracovanie dokumentácie z pohľadu procesov, metodiky, technických možností a inej dokumentácie. Podieľa sa na návrhu riešenia vrátane návrhu zmien procesov v oblasti biznis analýzy a analýzy softvérových riešení. Zodpovedá za výkon analýzy IS, koordináciu a dohľad nad činnosťou SW analytikov. • analyzuje požiadavky na informačný systém/softvérový systém, formálnym spôsobom zaznamenáva činnosti/procesy, vytvára analytický model systému, okrem analýzy realizuje aj návrh systému, ten vyjadruje návrhovým modelom. • Analytik informačných technológií pripravuje špecifikáciu cieľového systému od procesnej až po technickú rovinu. Mapuje a analyzuje existujúce podnikateľské a procesné prostredie, analyzuje biznis požiadavky na informačný systém, špecifikuje požiadavky na informačnú podporu procesov, navrhuje koncept riešenia a pripravuje podklady pre architektov a vývojárov riešenia, participuje na realizácii zmien, dohliada na realizáciu požiadaviek v cieľovom riešení, spolupracuje pri ich preberaní (akceptácie) používateľom. • Pri návrhu IT systémov využíva odbornú špecializáciu IT architektov a projektantov. Študuje a analyzuje dokumentáciu, požiadavky klientov, legislatívne a technické podmienky a možnosti zvyšovania efektívnosti a výkonnosti riadiacich a informačných procesov. Navrhuje a prerokúva koncepcie riešenia informačných systémov a analyzuje ich efekty a dopady. Zabezpečuje spracovanie analyticko-projektovej špecifikácie s návrhom dátových a objektových štruktúr a ich väzieb, užívateľského rozhrania a ostatných podkladov pre projektovanie nových riešení. • Spolupracuje na projektovaní a implementácii návrhov. Môže tiež poskytovať poradenstvo v oblasti svojej špecializácie. Zodpovedá za návrhovú (design) časť IT - pôsobí ako medzičlánok medzi používateľmi informačných systémov (biznis pohľad) a ich realizátormi (technologický pohľad).
Detailný popis rozsahu zodpovednosti, povinností a kompetencií	Zodpovedný za: • Vykonanie analýzy procesných a ďalších požiadaviek a vytvorenie špecifikácie súčasného alebo budúceho užívateľa softwaru („zákazníka") a následne navrhuje dizajn a programátorské riešenie. • Participáciu na vývoji nových, ale i vylepšovaní existujúcich aplikácií v rámci celého vývojového cyklu – systémová analýza, dizajn, kódovanie, užívateľské testovanie, implementácia, podpora, dokumentácia. Úzko spolupracuje aj s IT architektom. • Analýza potrieb zákazníka vrátane tvorby úplnej analytickej dokumentácie a vstupov do verejného obstarávania (VO). • Mapovanie požiadaviek do návrhu funkčných riešení. • Návrh a správa katalóg požiadaviek - registra požiadaviek riešenia • Analýza funkčných a nefunkčných požiadaviek, • Návrh fyzického a logického modelu, • Návrh testovacích scenárov, • V priebehu implementácie robí dohľad nad zhodou výstupov s pôvodným analytickým zadaním. • Zodpovednosť za dodržovanie správnej metodiky pri postupe analýzy • Definovanie akceptačných kritérií v projekte • Odsúhlasenie opisu produktov, ktoré predstavujú vstupy alebo výstupy (priebežné alebo konečné) úloh dodávateľov, alebo ktoré ich priamo ovplyvňujú a zabezpečovať akceptáciu produktov po ich dokončení

	• Priraďuje priority a poskytuje stanoviská používateľov na rozhodnutia Riadiaceho výboru projektu – k realizácii zmenových požiadaviek • Poskytuje merania aktuálneho stavu pre potreby porovnania s výsledkami projektu vzhľadom na realizáciu prínosov • Rieši požiadavky používateľov a konflikty iných priorít • Posúdenie prevádzkovo-infraštruktúrnej dokumentácie pred akceptáciou a prevzatím od dodávateľa • Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 85/2020 Z.z., Prílohou č.1 • Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

Projektová rola:	**BIZNIS VLASTNÍK**
Stručný popis:	• zodpovedá za proces - jeho výstupy i celkový priebeh poskytnutia služby alebo produktu konečnému užívateľovi. Kľúčová rola na strane zákazníka (verejného obstarávateľa), ktorá schvaľuje biznis požiadavky a zodpovedá za výsledné riešenie, prínos požadovanú hodnotu a naplnenie merateľných ukazovateľov. Úlohou tejto roly je definovať na užívateľa orientované položky (user-stories), ktoré budú zaradzované a prioritizované v produktovom zásobníku. Zodpovedá za priebežné posudzovanie vecných výstupov dodávateľa v rámci analýzy, návrhu riešenia vrátane DNR z pohľadu analýzy a návrhu riešenia aplikácii IS. • zodpovedný za schválenie funkčných a technických požiadaviek, potreby, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu. Definuje očakávania na kvalitu projektu, kvalitu projektových produktov, prínosy pre koncových používateľov a požiadavky na bezpečnosť. Definuje merateľné výkonnostné ukazovatele projektov a prvkov. Vlastník procesov schvaľuje akceptačné kritériá, rozsah a kvalitu dodávaných projektových výstupov pri dosiahnutí platobných míľnikov, odsúhlasuje spustenie výstupov projektu do produkčnej prevádzky a dostupnosť ľudských zdrojov alokovaných na realizáciu projektu.
Detailný popis rozsahu zodpovednosti, povinností a kompetencií	Zodpovedný za: • Realizáciu dohľadu nad súladom projektových výstupov s požiadavkami koncových používateľov. • Spoluprácu pri riešení odpovedí na otvorené otázky a riziká projektu. • Posudzovanie, pripomienkovanie, testovanie a protokolárne odsúhlasovanie projektových výstupov v príslušnej oblasti (v biznis procese) po vecnej stránke (najmä procesnej a legislatívnej) • Riešenie problémov a požiadaviek v spolupráci s odbornými garantmi, • Spoluprácu pri špecifikácii a poskytuje súčinnosť pri riešení zmenových požiadaviek • Schválenie funkčných a technických požiadaviek, potreby, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu z pohľadu používateľov koncového produktu • Definovanie očakávaní na kvalitu projektu, kritérií kvality projektových produktov, prínosov pre koncových používateľova požiadaviek na bezpečnosť, • Definovanie merateľných výkonnostných ukazovateľov projektov a prvkov, • Sledovanie a odsúhlasovanie nákladovosti, efektívnosti vynakladania finančných prostriedkov a priebežné monitorovanie a kontrolu odôvodnenia projektu (BC/CBA) • Schválenie akceptačných kritérií, • Riešenie problémov používateľov • Akceptáciu rozsahu a kvality dodávaných projektových výstupov pri dosiahnutí platobných míľnikov, • Vykonanie UX a UAT testovania • Odsúhlasenie spustenia výstupov projektu do produkčnej prevádzky, • Dostupnosť a efektívne využitie ľudských zdrojov alokovaných na realizáciu projektu, • Vykonávanie monitorovania a hodnotenia procesov v plánovaných intervaloch. • Poskytovanie vyjadrení k zmenovým požiadavkám, k ich opodstatnenosti a prioritizácii • Zisťovanie efektívneho spôsobu riadenia a optimalizácie zvereného procesu, vrátane analyzovanie všetkých vyskytujúcich sa nezhôd, • Okrem zvažovaní rizík prevádzkových alebo podporných procesov súčasne vlastník napomáha identifikovať príležitosti, • Zlepšovanie a optimalizáciu procesov v spolupráci s ďalšími prepojenými vlastníkmi procesov a manažérom kvality, • Odsúhlasenie akceptačných protokolov zmenových konaní • 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
Poznámka	Rola **VLASTNÍK PROCESOV je biznis vlastník,** ide o kľúčovú rolu v rámci projektového tímu.

Projektová rola:	**MANAŽÉR KVALITY**
Stručný popis:	• zodpovedá za priebežné vyžadovanie, hodnotenie a kontrolu kvality (vecnej aj formálnej) počas celého projektu. Je zodpovedný za úvodné nastavenie pravidiel riadenia kvality a za následné dodržiavanie a kontrolu kvality jednotlivých projektových výstupov. Sleduje a hodnotí kvalitatívne ukazovatele projektových výstupov a o zisteniach informuje projektového manažéra objednávateľa formou pravidelných alebo nepravidelných správ/záznamov. • plánuje, koordinuje, riadi a kontroluje systém manažérstva kvality, monitoruje a meria procesy a identifikuje príležitosti na trvalé zlepšovanie systému manažérstva kvality v organizácii v súlade s platnými normami. Zabezpečuje tvorbu cieľov a koncepcie kvality, vrátane kontroly ich plnenia a vykonáva interné a externé audity kvality v súlade s plánom. • Počas celej doby realizácie projektu zabezpečuje zhodu kvality projektových výstupov s požiadavkami. Realizuje postupy riadenia kvality tak, aby výsledkom boli projektové výstupy spĺňajúce požiadavky objednávateľa. Kontroluje, či sa riadenie a proces zabezpečenia kvality vykonáva správnym spôsobom, v správnom čase a správnymi osobami.
Detailný popis rozsahu zodpovednosti, povinností a kompetencií	Zodpovedný za: • Návrh a zavádzanie do praxe postupov, techník, nástrojov a pravidiel, ktoré maximalizujú efektivitu práce a kvalitatívne parametre vývoja softwaru/produktu/IS, resp. IT projektu • Definovanie politiky kvality (stratégie kvality), meranie kvality, analýzu a spracovanie plánov kvality, • Riadenie a monitorovanie dosahovania cieľov kvality, • Špecifikáciu požiadaviek na kvalitu vyvíjaných funkcionalít systému • Špecifikáciu požiadaviek pre ďalší rozvoj, • Definovanie akceptačných kritérií • Zabezpečenie súladu so štandardmi, normami, právnymi požiadavkami, požiadavkami užívateľov a prevádzkovateľov systémov, • Posúdenie BC/CBA – odôvodení projektu • Kontrolu kvalitu plnenia vecných požiadaviek definovaných v Zmluve s dodávateľom alebo v požiadavkách na zmenu, • Akceptáciu splnenia vecných a kvalitatívnych požiadaviek v projekte svojím podpisom na akceptačnom protokole pri odovzdávaní jednotlivých fáz projektu/čiastkových projektov alebo pri odovzdávaní zmien vykonaných v rámci zmenových konaní, • Aktívnu účasť rokovaniach a participáciu na riešení vecných požiadaviek členov projektového tímu, • Monitoring a vyhodnocovanie kvality údajov a návrh nápravných opatrení za účelom zabezpečenia správnosti a konzistentnosti údajov • Definovanie postupov, navrhovanie a vyjadrovanie sa k plánom testov a testovacích scenárov • Analyzovanie výsledkov testovania. • Kontrolu plnenia projektových úloh a časového harmonogramu projektu • Kontrolu plnenia finančného plánu projektu • Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 85/2020 Z.z., Prílohou č.1 • Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

Projektová rola:	**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: a) § 20 zákona č.69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov b) ustanovení zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
Detailný popis rozsahu zodpovednosti, povinností a kompetencií	Zodpovedný za: • špecifikovanie štandardov, princípov a stratégií v oblasti 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

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

10. PRÍLOHY

Príloha : Zoznam rizík a závislostí (Excel):

Koniec dokumentu