PRÍSTUP K PROJEKTU

Vzor pre manažérsky výstup P-03

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	9.10.2024	Prípravná fáza projetu	Mgr. Miroslav Odor

2. ÚČEL DOKUMENTU

V súlade s Vyhláškou 401/2023 Z.z. je dokument P-03 Prístup k projektu určený na rozpracovanie detailných informácií prípravy projektu z pohľadu aktuálneho stavu, budúceho stavu a navrhovaného riešenia.

Dokument Prístup k projektu v zmysle vyššie uvedenej vyhlášky a požiadaviek výzvy: Podpora v oblasti kybernetickej a informačnej bezpečnosti, číslo výzvy: PSK-MIRRI-616-2024-DV-EFRR (ďalej len „výzva“) bude obsahovať opis navrhovaného riešenia, architektúru riešenia projektu na úrovni biznis vrstvy, aplikačnej vrstvy, dátovej vrstvy, technologickej vrstvy, infraštruktúry navrhovaného riešenia, bezpečnostnej architektúry, špecifikáciu údajov spracovaných v projekte, čistenie údajov, prevádzku a údržbu výstupov projektu, prevádzkové požiadavky, požiadavky na zdrojové kódy. Zároveň opisuje aj implementáciu projektu a preberanie výstupov projektu.

Manažérske produkty – vrátane prístupu k projektu – 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. POPIS NAVRHOVANÉHO RIEŠENIA

Navrhované riešenie vychádza z aktuálnych zistení posledného auditu kybernetickej bezpečnosti MŠVVaM SR. Ten definuje aktuálny stav a potreby, ktoré je nevyhnutné riešiť pre dosiahnutie súladu úrovne kybernetickej a informačnej bezpečnosti (ďalej len KIB) so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len "zákon o kybernetickej bezpečnosti), Zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len "zákon o ISVS"), vyhláškou 362/2018 Z.z. o obsahu bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len vyhláška č. 362/2018 Z. z.) a ďalšími súvisiacimi predpismi.

V rámci projektového zámeru boli stanovené nasledovné ciele a spôsob ich riešenia:

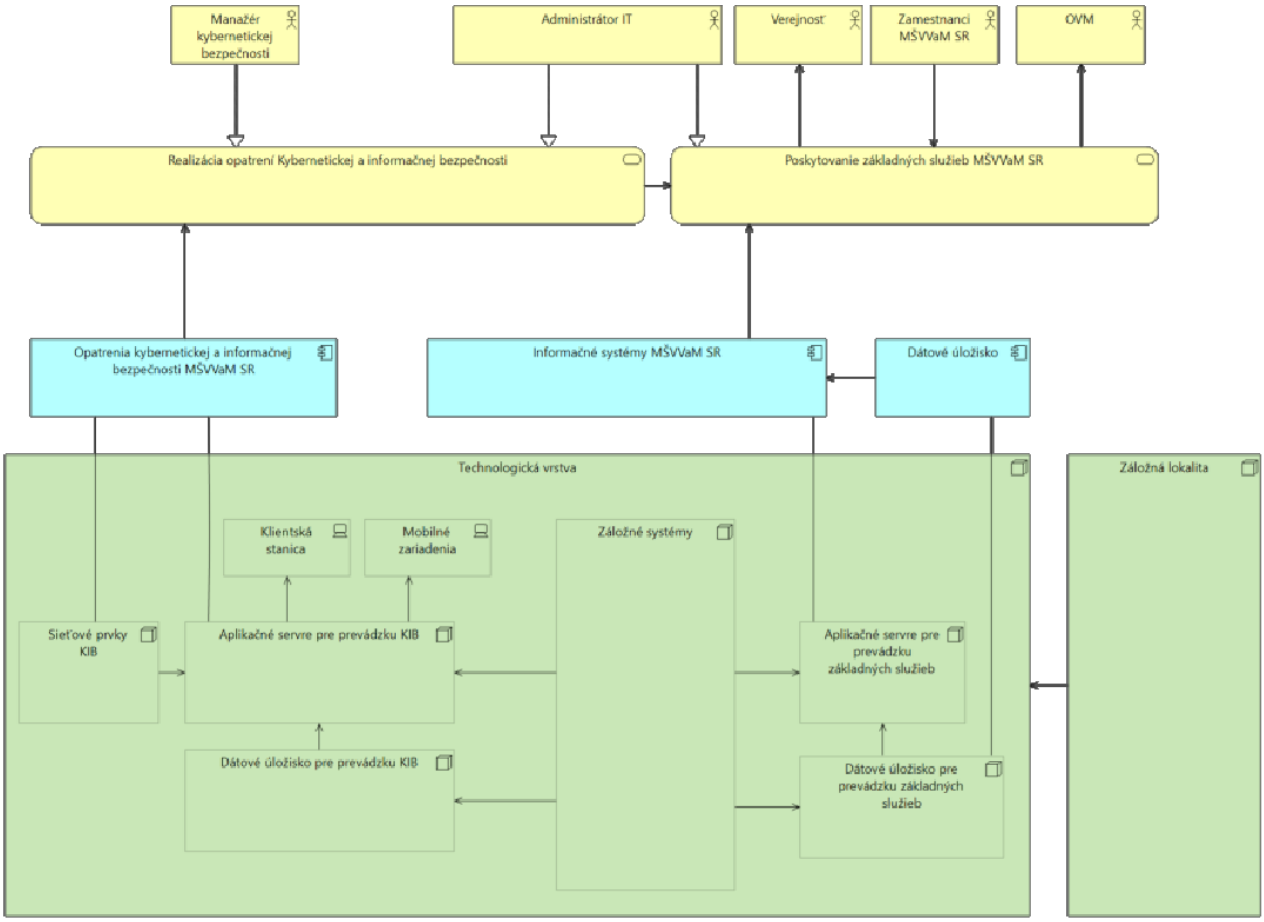
ID	Názov cieľa	Názov strategického cieľa*	Spôsob realizácie strategického cieľa
1	Zavedenie správy privilegovaných účtov Cieľ realizovaný v zmysle oprávnenej oblasti: Riadenie prístupov	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	• Dodanie softvérového vybavenia na správu privilegovaných účtov • Realizácia implementačných prác pri zavedení správy privilegovaných účtov
2.	Zavedenie aplikácie na správu a aktualizáciu bezpečnostnej dokumentácie Cieľ realizovaný v zmysle oprávnenej oblasti: Bezpečnosť pri prevádzke informačných systémov a sietí	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	• Dodanie Aplikácie na správu a aktualizáciu bezpečnostnej dokumentácie • Realizácia implementačných prác pri zavedení Aplikácie na správu a aktualizáciu bezpečnostnej dokumentácie
3.	Zabezpečenie ochrany užívateľských zariadení pred kybernetickými hrozbami	Dôveryhodný štát pripravený na hrozby	• Prechod na licencie ESET PROTECT Enterprise

	Cieľ realizovaný v zmysle oprávnenej oblasti: Ochrana proti škodlivému kódu	(Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	• 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

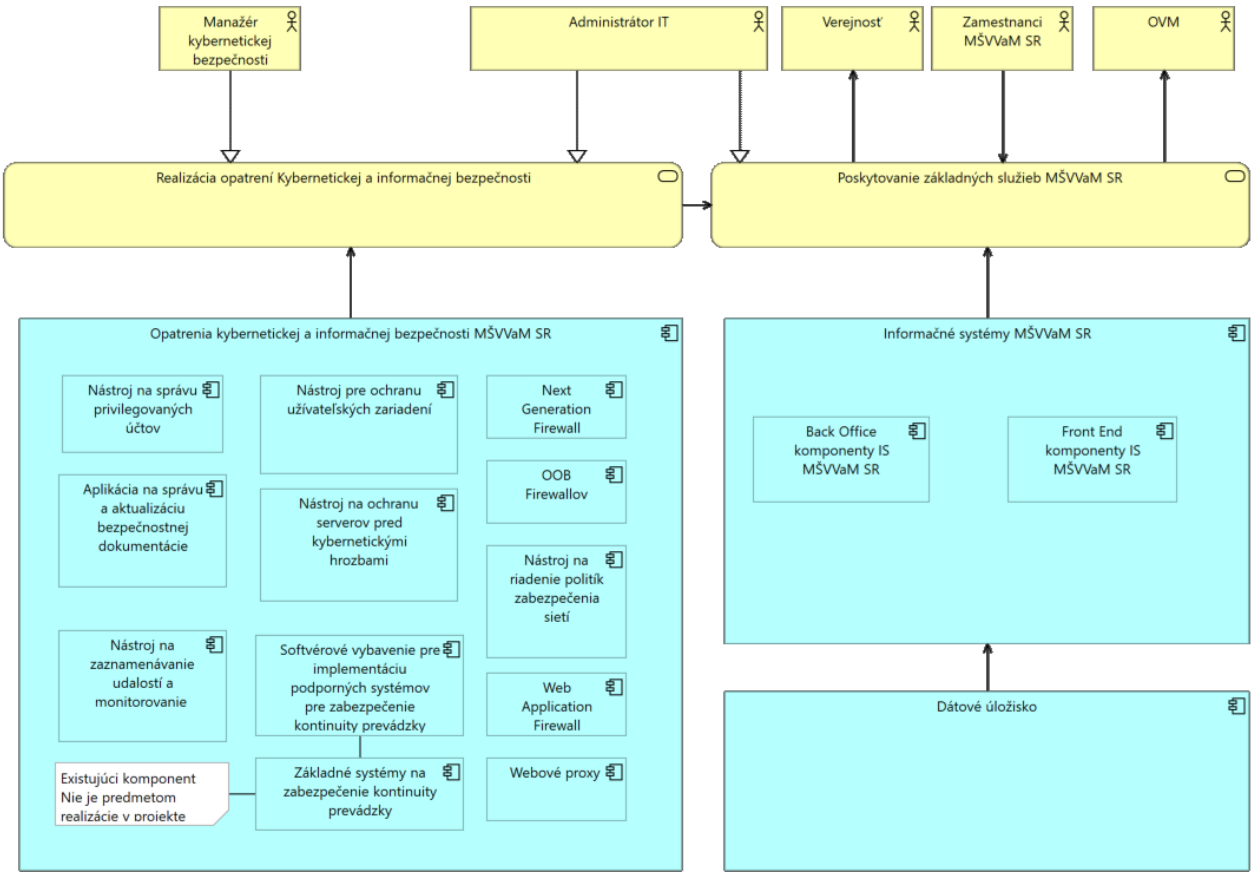
4. ARCHITEKTÚRA RIEŠENIA PROJEKTU

Architektúra celého riešenia je rámcová tak, aby bolo z projektu zrejmé, ktoré komponenty v rámci realizácie projektu budú vytvorené, aktualizované alebo rozšírené a tým budú realizované opatrenia KIB v rámci projektu.

Primárne opatrenia kybernetickej bezpečnosti chránia IS MŠVVaM SR, ktoré sú určené na prevádzkovanie ZS MŠVVaM SR. Z vyššie definovaných spôsobov realizácie cieľov (viď kapitola 3 Popis navrhovaného riešenia) je zrejmé, o aké komponenty zabezpečenia pôjde.



Obrázok 1: Celková architektúra riešenia



Obrázok 2: Aplikačná architektúra riešenia

4.1 Biznis vrstva

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

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 ISVS 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.

4.1.1 Prehľad koncových služieb – budúci stav:

Projekt nerealizuje koncové služby pre občanov a podnikateľov. Realizáciou projektu dochádza k zavedeniu opatrení kybernetickej a informačnej bezpečnosti (ďalej len KIB), ktoré zabraňujú kybernetickým útokom a na základe toho chránia prevádzku ostatných koncových služieb.

Z toho vyplýva, že v rámci projektu nevznikne žiadna nová koncová služba v zmysle zákona o ISVS.

4.1.2 Jazyková podpora a lokalizácia

Projekt bude realizovaný v podobe dokumentov (politiky, plány, stratégie atď.), ktoré budú akceptované výhradne v slovenskom jazyku. Implementované softvérové riešenia budú akceptované v slovenskej, českej alebo na základe súhlasu MŠVVaM SR v anglickej mutácií. Dodané softvérové riešenia alebo hardvérové komponenty musia mať návod v slovenskom jazyku. Projektová dokumentácia bude vyhotovovaná v slovenskom alebo českom jazyku. Výstupy z prevádzky systémov budú akceptované v slovenskom, vo výnimočných prípadoch anglickom jazyku, niektoré čiastkové výstupy (napr. logy incidendov) sú akceptované v podobe skriptov, ktoré musí byť možné transformovať do používateľsky zrozumiteľného jazyka resp. zabezpečiť ich vhodnú interpretáciu.

4.2 Aplikačná vrstva

Aplikačná vrstva bude realizovaná súborom opatrení KIB, ktoré budú ochraňovať IS zabezpečujúce primárne prevádzku ZS. V aplikačnej vrstve je potrebné uvažovať o FrontEnd (verejných) častiach základnej služby a Back-Office (neverejných častiach) ZS.

V prípade MŠVVaM SR budú všetky komponenty projektu realizované ako opatrenia inštalované in situ v rámci MŠVVaM SR.

4.2.1 Rozsah informačných systémov – AS IS

V nasledujúcej tabuľke uvádzame ISVS, ktoré zabezpečujú prevádzku ZS MŠVVaM SR a budú primárne chránené proti incidentom KIB po ukončení projektu:

Kód ISVS *(z MetaIS)*	**Názov ISVS**	**Modul ISVS** *(zaškrtnite ak ISVS je modulom)*	**Stav IS VS** (AS IS)	**Typ IS VS**	**Kód nadradeného ISVS** *(v prípade zaškrtnutého checkboxu pre modul ISVS)*
isvs_376	Centrálna elektronická prihláška na vysoké školy	☐	Prevádzkovaný a plánujem rozvíjať	Agendový	
isvs_6092	RIS - Rezortný informačný systém	☐	Prevádzkovaný a plánujem rozvíjať	Agendový	
isvs_6712	Centrálny register zamestnancov VŠ	☐	Prevádzkovaný a plánujem rozvíjať	Agendový	

Kód ISVS *(z MetaIS)*	**Názov ISVS**	**Modul ISVS** *(zaškrtnite ak ISVS je modulom)*	**Stav IS VS** (AS IS)	**Typ IS VS**	**Kód nadradeného ISVS** *(v prípade zaškrtnutého checkboxu pre modul ISVS)*
isvs_374	Centrálny register študentov vysokých škôl	☐	Prevádzkovaný a plánujem rozvíjať	Agendový	
isvs_6301	Portál Ministerstva školstva, vedy, výskumu a športu SR	☐	Prevádzkovaný a plánujem rozvíjať	Prezentačný	

4.2.2 Rozsah informačných systémov – TO BE

V rámci projektu nevznikne nový ISVS v zmysle definície zákona o ISVS. Vznikne súbor opatrení, ktorý bude chrániť existujúce ISVS (ich zoznam viď predchádzajúca kapitola) – k nim je vytvorený vzťah realizovaného projektu.

4.2.3 Využívanie nadrezortných a spoločných ISVS – AS IS

Projekt nebude využívať nadrezortné a spoločne ISVS .

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

Projekt nebude integrovaný na ISVS a nadrezortné ISVS – spoločné moduly podľa zákona č. 305/2013 o e-Governmente.

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

Projekt nebude integrovaný na iné ISVS.

4.2.6 Aplikačné služby pre realizáciu koncových služieb – TO BE

V rámci projektu nevznikne žiadna nová aplikačná služba.

4.2.7 Aplikačné služby na integráciu – TO BE

Predmetom realizácie nebudú žiadne služby určené na integráciu v rámci TO BE stavu.

4.2.8 Poskytovanie údajov z ISVS do IS CSRÚ – TO BE

Projekt nebude poskytovať údaje z ISVS do IS CSRU.

4.2.9 Konzumovanie údajov z IS CSRU – TO BE

Projekt nebude konzumovať údaje z IS CSRU.

4.3 Dátová vrstva

4.3.1 Údaje v správe organizácie

Projekt resp. ním realizovaný ISVS nebude priamo zabezpečovať správu údajov MŠVVaM SR, bude spravovať iba údaje nevyhnutné na zabezpečenie KIB MŠVVaM SR (napríklad údaje logov zo SIEM, informácie o riešení incidentov KIB, zoznam oprávnení a pod.).
Z toho dôvodu neuvádzame namapovanú štruktúru údajov v správe MŠVVaM SR.

4.3.2 Dátový rozsah projektu - Prehľad objektov evidencie - TO BE

V rámci realizovaného projektu nevzniknú nové objekty evidencie tak, ako vznikajú v prípade štandardných informačných systémov. Predmetom evidencie nebudú napríklad občania resp. informácie o nich atď. Systém bude viesť evidenciu prístupov a oprávnení, v

rámci služby SIEM budú vznikať záznamy o incidentoch a tieto budú vyhodnocované a na základe nich budú prebiehať priamo reakcie na kybernetické incidenty - poskytovateľom služby SOC v súčinnosti so zástupcami MŠVVaM SR.

4.3.3 Referenčné údaje

V rámci projektu nebudú využívané referenčné údaje ani projekt nebude poskytovať referenčné údaje.

4.3.3.1 OBJEKTY EVIDENCIE Z POHĽADU PROCESU ICH VYHLÁSENIA ZA REFERENČNÉ

V rámci projektu nebudú spravované údaje určené na konzumovanie alebo poskytovanie do/z CSRU.

4.3.3.2 IDENTIFIKÁCIA ÚDAJOV PRE KONZUMOVANIE ALEBO POSKYTOVANIE ÚDAJOV DO/Z CSRU

V rámci projektu nebudú spravované údaje určené na konzumovanie alebo poskytovanie do/z CSRU.

4.3.4 Kvalita a čistenie údajov

4.3.4.1 ZHODNOTENIE OBJEKTOV EVIDENCIE Z POHĽADU DÁTOVEJ KVALITY

Predmetom projektu nebude hodnotenie kvality ani čistenie údajov.

4.3.4.2 ROLY A PREDBEŽNÉ PERSONÁLNE ZABEZPEČENIE PRI RIADENÍ DÁTOVEJ KVALITY

Nakoľko v rámci projektu nebudú prebiehať procesy hodnotenia kvality a čistenia údajov, nebudú obsadené roly na personálne zabezpečenie pri riadení dátovej kvality.

4.3.5 Otvorené údaje

V rámci projektu nebudú vytvárané otvorené údaje.

4.3.6 Analytické údaje

V rámci projektu nebudú vytvárané analytické údaje.

4.3.7 Moje údaje

V rámci projektu nebudú vytvárané moje údaje.

4.3.8 Prehľad jednotlivých kategórií údajov

Predmetom realizácie projektu nebudú žiadne údaje, ktoré by boli referenčnými, spadali by do kategórie “Moje údaje”, “Otvorené údaje” a tiež nebudú poskytované ako analytické údaje.

4.4 Technologická vrstva

4.4.1 Prehľad technologického stavu - AS IS

S ohľadom na inštrukcie MIRRI SR neuvádzame podrobný prehľad technologického stavu AS IS.

Konštatujeme, že z pohľadu zabezpečenia KIB je potrebné AS IS stav doplniť tak, aby bol zabezpečený súlad opatrení KIB s požiadavkami zákona o kybernetickej bezpečnosti

4.4.2 Požiadavky na výkonnostné parametre, kapacitné požiadavky – TO BE

Parameter	Jednotky	Predpokladaná hodnota	Poznámka
Počet interných používateľov	Počet	700	
Počet súčasne pracujúcich interných používateľov v špičkovom zaťažení	Počet	900	

Počet externých používateľov (internet)	Počet	99 000	
Počet externých používateľov používajúcich systém v špičkovom zaťažení	Počet	90 000	Maximálny počet používateľov – interných aj externých, ktorí sa môžu prihlásiť naraz k základným službám či už ako poskytovatelia (zamestnanci) alebo ako konzumenti
Počet transakcií (podaní, požiadaviek) za obdobie	Počet/obdobie	Irelevantné	
Objem údajov na transakciu	Objem/transakcia	1 MB/transakcia	Maximálna predpokladaná hodnota
Objem existujúcich kmeňových dát	Objem	irelevantné	

4.4.3 Návrh riešenia technologickej architektúry

Technologicky pôjde o realizáciu nasledovných opatrení:

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

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

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.

Zabezpečenie ochrany užívateľských zariadení pred kybernetickými hrozbami

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

- zvýšená ochrana proti spusteniu škodlivého kódu na pracovných staniciach, notebookoch a mobilných zariadeniach pomocou Microsoft Defender for Endpoint a Microsoft Defender for Cloud Apps
- kontrola externých zdieľaní na škodlivý kód pomocou Safe links a Safe attachments
- testovanie a simulácia prienikov škodlivého kódu
- Kontrola prístupu užívateľov a detekcia kompromitovaných účtov pomocou rozšírení Entra ID P2
- rozšírenie kontroly prístupu k službám Microsoft 365 pomocou podmieneného prístupu na základe správania užívateľa
- zvýšenie ochrany dokumentov vynútením ich automatickej klasifikácie pomocou Information protection P2

V rámci dodávky budú realizované nasledovné činnosti:

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

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

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

Rozšírenie logovacieho systému o korelácie a automatizáciu

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

Implementácia podporných systémov pre zabezpečenie kontinuity prevádzky

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 Datacenter 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

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

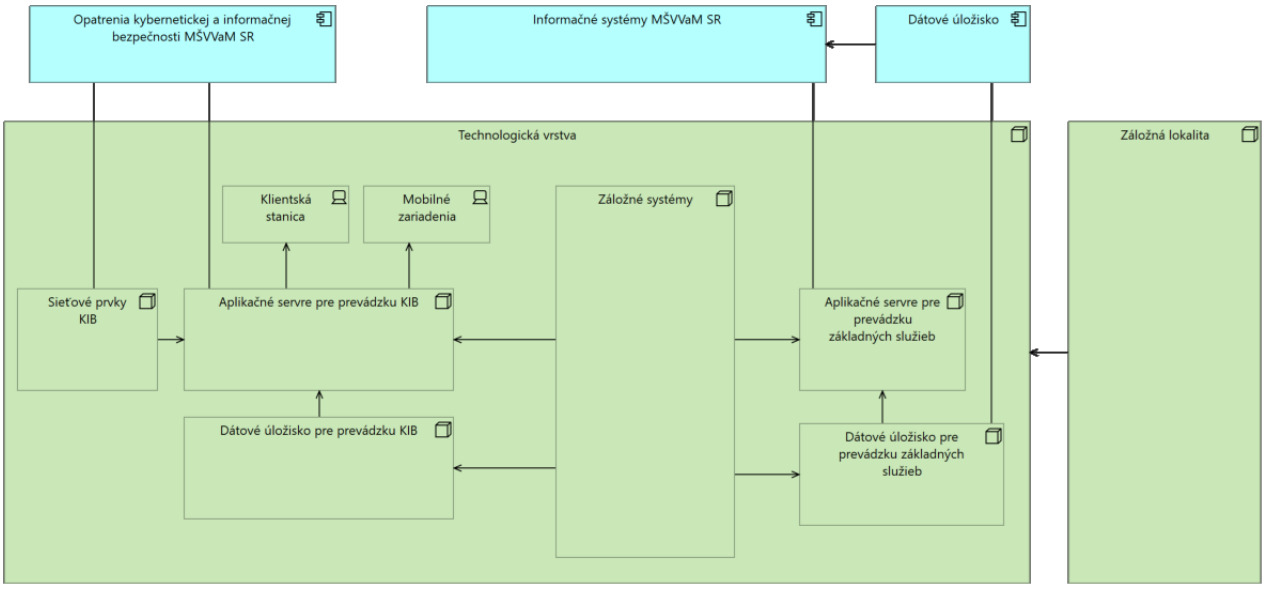
Predmetom zákazky je poskytnúť verejnému obstarávateľovi cenovú ponuku pre vykonanie auditu kybernetickej bezpečnosti v prostredí *Ministerstva školstva, vedy, výskumu a športu Slovenskej republiky*, ktorý musí byť realizovaný podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení 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

Fáza auditu	***Termín***
Nastavenie a výkon auditu kybernetickej bezpečnosti	November 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



Obrázok 3: Technologická architektúra

4.4.4 Využívanie služieb z katalógu služieb vládneho cloudu

Projekt nebude využívať služby vládneho cloudu.

4.5 Bezpečnostná architektúra

V súčasnosti - ako vyplýva z projektového zámeru - nie sú opatrenia KIB MŠVVaM SR - v súlade s požiadavkami príslušných predpisov. Navrhovaná architektúra riešenia t.j. dosiahnutie TO BE stavu bude znamenať dosiahnutie súladu opatrení s nasledovnou legislatívou:

- Zákon č. 95/2019 Z.z. o informačných technológiách vo verejnej správe
- Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti
- Zákon č. 45/2011 Z.z. o kritickej infraštruktúre
- vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy
- vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy
- vyhláška Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov
- Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
- Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

5. ZÁVISLOSTI NA OSTATNÉ ISVS / PROJEKTY

Projekt nie je závislý od iných ISVS alebo projektov.

6. ZDROJOVÉ KÓDY

MŠVVaM SR plánuje pri obstarávaní jednotlivých súčastí projektu, pri ktorých môžu vzniknúť zdrojové kódy postupovať v zmysle vzoru Zmluvy o dielo. Zmluvnú úpravu predkladáme nasledujúcu:

- Zhotoviteľ je povinný pri akceptácii Informačného systému odovzdať Objednávateľovi funkčné vývojové a produkčné prostredie, ktoré je súčasťou Informačného systému.
- Zhotoviteľ je povinný pri akceptácii Informačného systému alebo jeho časti odovzdať Objednávateľovi Vytvorený zdrojový kód v jeho úplnej aktuálnej podobe, zapečatený, na neprepisovateľnom technickom nosiči dát s označením časti a verzie Informačného systému, ktorej sa týka. Za odovzdanie Vytvoreného zdrojového kódu Objednávateľovi sa na účely tejto Zmluvy o dielo rozumie odovzdanie technického nosiča dát Oprávnenej osobe Objednávateľa. O odovzdaní a prevzatí technického nosiča dát bude oboma Zmluvnými stranami spísaný a podpísaný preberací protokol.

- Informačný systém (Dielo) v súlade s Technickou špecifikáciou obsahuje od zvýšku Diela oddeliteľný modul (časť) vytvorený Zhotoviteľom pri plnení tejto Zmluvy o dielo, ktorý je bez úpravy použiteľný aj tretími osobami, aj na iné alebo podobné účely, ako je účel vyplývajúci z tejto Zmluvy o dielo Vytvorený zdrojový kód Informačného systému vrátane jeho dokumentácie bude prístupný v režime podľa § 31 ods. 4 písm. b) Vyhlášky č. 78/2020 (s obmedzenou dostupnosťou pre orgán vedenia a orgány riadenia v zmysle Zákona o ITVS – vytvorený zdrojový kód je dostupný len pre orgán vedenia a orgány riadenia). Pre zamedzenie pochybností uvádzame, že sa jedná len o zdrojový kód ktorý Zhotoviteľ vytvoril, alebo pozmenil v súvislosti s realizáciou diela. Objednávateľ je oprávnený sprístupniť Vytvorený zdrojový kód okrem orgánov podľa predchádzajúcej vety aj tretím osobám, ale len na špecifický účel, na základe riadne uzatvorenej písomnej zmluvy o mlčanlivosti a ochrane dôverných informácií.
- Ak je medzi zmluvnými stranami uzatvorená SLA zmluva, od prevzatia Informačného systému sa prístup k vytvorenému zdrojovému kódu vo vývojovom a produkčnom prostredí, vrátane nakladania s týmto zdrojovým kódom, začne riadiť podmienkami dohodnutými v SLA zmluve. Vytvorený zdrojový kód musí byť v podobe, ktorá zaručuje možnosť overenia, že je kompletný a v správnej verzii, t. j. v takej, ktorá umožňuje kompiláciu, inštaláciu, spustenie a overenie funkcionality, a to vrátane kompletnej dokumentácie zdrojového kódu (napr. interfejsov a pod.) takéhoto Informačného systému alebo jeho časti. Zároveň odovzdaný Vytvorený zdrojový kód musí byť pokrytý testami (aspoň na 90%) a dosahovať rating kvality (statická analýza kódu) podľa CodeClimate/CodeQLa pod. (minimálne stupňa B).
- Pre zamedzenie pochybností, povinnosti Zhotoviteľa týkajúce sa Vytvoreného zdrojového kódu platí i na akékoľvek opravy, zmeny, doplnenia, upgrade alebo update Vytvoreného zdrojového kódu a/alebo vyššie uvedenej dokumentácie, ku ktorým dôjde pri plnení tejto Zmluvy o dielo alebo v rámci záručných opráv. Vytvorené zdrojové kódy budú vytvorené vyexportovaním z produkčného prostredia a budú odovzdané Objednávateľovi na elektronickom médiu v zapečatenom obale. Zhotoviteľ je povinný umožniť Objednávateľovi pri odovzdávaní Vytvoreného zdrojového kódu, pred zapečatením obalu, skontrolovať v priestoroch Objednávateľa prítomnosť Vytvoreného zdrojového kódu na odovzdávanom elektronickom médiu.
- Nebezpečenstvo poškodenia zdrojových kódov prechádza na Objednávateľa momentom prevzatia Informačného systému alebo jeho časti, pričom Objednávateľ sa zaväzuje uložiť zdrojové kódy takým spôsobom, aby zamedzil akémukoľvek neoprávnenému prístupu tretej osoby. Momentom platnosti SLA zmluvy umožní Objednávateľ poskytovateľovi, za predpokladu, že to je nevyhnutné, prístup k Vytvorenému zdrojovému kódu výlučne na účely plnenia povinností z uzatvorenej SLA zmluvy.

Ďalej uvádzame postupy, v zmysle ktorých bude narábané so zdrojovým kódom

Centrálny repozitár zdrojových kódov: https://www.zakonypreludi.sk/zz/2020-78/znenie-20200501#p31

Overenie zdrojového kódu s cieľom jeho prepoužitia: https://www.zakonypreludi.sk/zz/2020-85/znenie-20200501#p7-3-c

Spôsoby zverejňovania zdrojového kódu: https://www.zakonypreludi.sk/zz/2020-85/znenie-20200501#p8-9

Inštrukcie k EUPL licenciám: https://joinup.ec.europa.eu/sites/default/files/inline-files/EUPL%201_1%20Guidelines%20SK%20Joinup.pdf

Uvedeným spôsobom obstarávania dôjde k zamedzeniu „Vendor lock-in" v súlade so Zákonom o ISVS.

7. PREVÁDZKA A ÚDRŽBA

Požadované SLA na služby systémovej a aplikačnej podpory – servisné služby vzťahujúce sa na produkčné a testovacie prostredie IS
Úrovne podpory používateľov: Help Desk bude realizovaný cez 3 úrovne podpory, s nasledujúcim označením:

- L1 podpory IS (Level 1, priamy kontakt zákazníka) - jednotný kontaktný bod verejného obstarávateľa.
- L2 podpory IS (Level 2, postúpenie požiadaviek od L1) - vybraná skupina garantov, so znalosťou IS (zabezpečuje prevádzkovateľ IS – verejný obstarávateľ).
- L3 podpory IS (Level 3, postúpenie požiadaviek od L2) - na základe zmluvy o podpore IS (zabezpečuje úspešný uchádzač).

Definície:

- Podpora L1 (podpora 1. stupňa) - začiatočná úroveň podpory, ktorá je zodpovedná za riešenie základných problémov a požiadaviek koncových užívateľov a ďalšie služby vyžadujúce základnú úroveň technickej podpory. Základnou funkciou podpory 1. stupňa je zhromaždiť informácie, previesť základnú analýzu a určiť príčinu problému a jeho klasifikáciu. Typicky sú v úrovni L1 riešené priamočiare a jednoduché problémy a základné diagnostiky, overenie dostupnosti jednotlivých vrstiev infraštruktúry (sieťové, operačné, vizualizačné, aplikačné atď.) a základné užívateľské problémy (typicky zabudnutie hesla), overovanie nastavení SW a HW atď.
- Podpora L2 (podpora 2. stupňa) – riešiteľské tímy s hlbšou technologickou znalosťou danej oblasti. Riešitelia na úrovni Podpory L2 nekomunikujú priamo s koncovým užívateľom, ale sú zodpovední za poskytovanie súčinnosti riešiteľom 1. úrovne podpory pri riešení eskalovaného hlásenia, čo mimo iného obsahuje aj spätnú kontrolu a podrobnejšiu analýzu zistených dát odovzdaných riešiteľmi 1. úrovne podpory. Výstupom takejto kontroly môže byť potvrdenie, upresnenie, alebo prehodnotenie hlásenia v závislosti na potrebách Objednávateľa. Primárnym cieľom riešiteľov na úrovni Podpory L2 je dostať Hlásenie čo najskôr pod kontrolu a následne ho vyriešiť - s možnosťou eskalácie na vyššiu úroveň podpory – Podpora L3.
- Podpora L3 (podpora 3. stupňa) - Podpora 3. stupňa predstavuje najvyššiu úroveň podpory pre riešenie tých najobtiažnejších Hlásení, vrátane vykonávania hĺbkových analýz a riešenie extrémnych prípadov.
- Riešenie incidentov – SLA parametre Za incident je považovaná chyba IS, t.j. správanie sa v rozpore s prevádzkovou a používateľskou dokumentáciou IS. Za incident nie je považovaná chyba, ktorá nastala mimo prostredia IS napr. výpadok poskytovania konkrétnej služby. Označenie závažnosti incidentu:

Závažnosť incidentu	Popis naliehavosti incidentu
Kritická, Bezpečnostná	Kritické chyby, ktoré spôsobia úplné zlyhanie systému ako celku a nie je možné používať ani jednu jeho časť, nie je možné poskytnúť požadovaný výstup z IS.
Bežná	Chyby a nedostatky, ktoré spôsobia čiastočné obmedzenia používania systému
Nekritická	Kozmetické a drobné chyby.

Vyžadované reakčné doby:

Označenie závažnosti incidentu	Reakčná doba od nahlásenia incidentu po začiatok riešenia incidentu	Doba konečného vyriešenia incidentu od nahlásenia incidentu (DKVI)	Spoľahlivosť (počet incidentov za mesiac)
Bežná	Do 24 hodín	48 hodín	5
Kritická	Do 12 hodín	24 hodín	3
Nekritická	Do 48 hodín	Vyriešené a nasadené v rámci plánovaných releasov	
Bezpečnostná	Do 12 hodín	24 hodín	1

Požiadavky na hlásenie Incidentov sa spracúvajú v rámci časového pokrytia od 8:00 do 16:00.

- Reakčná doba je čas medzi nahlásením incidentu verejným obstarávateľom (vrátane užívateľov IS, ktorí nie sú v pracovnoprávnom vzťahu s verejným obstarávateľom) na helpdesk úrovne L3 a jeho prevzatím na riešenie.
- DKVI znamená obnovenie štandardnej prevádzky – čas medzi nahlásením incidentu verejným obstarávateľom a vyriešením incidentu úspešným uchádzačom (do doby, kedy je funkčnosť prostredia znovu obnovená v plnom rozsahu). Do tejto doby sa nezarátava čas potrebný na nevyhnutnú súčinnosť verejného obstarávateľa, ak je potrebná pre vyriešenie incidentu. V prípade potreby je úspešný uchádzač oprávnený požadovať od verejného obstarávateľa schválenie riešenia incidentu.
- Maximálny počet incidentov za kalendárny mesiac. Každá ďalšia chyba nad stanovený limit spoľahlivosti sa počíta ako začatý deň omeškania bez odstránenia vady alebo incidentu. Duplicitné alebo technicky súvisiace incidenty (zadané v rámci jedného pracovného dňa, počas pracovného času 8 hodín) sú považované ako jeden incident.

Incidenty nahlásené verejným obstarávateľom úspešnému uchádzačovi v rámci testovacieho prostredia

- Majú závažnosť incidentu nekritickú a nižšiu
- Vzťahujú sa výhradne k dostupnosti testovacieho prostredia
- Za incident na testovacom prostredí sa nepovažuje incident vztiahnutý k práve testovanej funkcionalite

Vyššie uvedené SLA parametre nebudú použité pre nasledovné služby:

- Služby systémovej podpory na požiadanie (nad paušál)

Služby realizácie aplikačných zmien vyplývajúcich z legislatívnych a metodických zmien (nad paušál)

8. POŽIADAVKY NA PERSONÁL

Výzva definuje požiadavky na IT odborníkov participujúcich v rámci projektu – má ísť minimálne o manažéra kybernetickej bezpečnosti. Aby bol dodržaný súlad realizácie projektu s vyhláškou č.401/2023 Z.z. bude zostavený nasledovný projektový tím objednávateľa:

- kľúčový používateľ - PhDr. Mgr. Ľubomír Nebeský, PhD.
- IT architekt – Martin Bokor
- IT analytik - Mgr. Miroslav Odor
- biznis vlastník - Ing. Martin Horňák
- manažér kvality – JUDr. Jozef Stopka
- manažér kybernetickej a informačnej bezpečnosti - Mgr. Miroslav Odor
- projektový manažér (pre účely realizácie) - JUDr. Ing. Jana Barjaková

ID	Meno a Priezvisko	Pozícia	Oddelenie	Rola v projekte
1.	PhDr. Mgr. Ľubomír Nebeský, PhD.	GR kancelárie GTSÚ	MŠVVaM SR	kľúčový používateľ
2.	Martin Bokor	IT špecialista - architekt pre SHMÚ	SHMÚ IT oddelenie	IT architekt
	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

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.

Pracovné náplne členov tímu

V zmysle Vyhlášky 401/2023 Z.z. o riadení projektov a zmenových požiadaviek v prevádzke a požiadaviek Výzvy budú obsadené vyššie uvedené role v projektovom tíme. Náplne práce a požiadavky na členov tímu sú nasledovné:

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

9. IMPLEMENTÁCIA A PREBERANIE VÝSTUPOV PROJEKTU

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.

Implementácia a preberanie výstupov projektu bude prebiehať v zmysle nasledovného harmonogramu:

- Dodávka všetkých hardvérových a softvérových komponentov predmetu plnenia bude realizovaná v rámci realizačnej fázy projektu Nákup technických prostriedkov, programových prostriedkov a služieb (v harmonograme označovaný skratkou „Nákup“): maximálne 150 dní od dátumu odoslania písomného pokynu na začatie realizácie realizačnej fázy Nákup technických prostriedkov, programových prostriedkov a služieb.
- Realizačná fáza projektu „Analýza a dizajn“ bude prebiehať 8 mesiacov od dátumu odoslania písomného pokynu na začatie realizácie.
- Realizačná fáza projektu „Implementácia a testovanie“ bude prebiehať 14 mesiacov od ukončenia realizačnej fázy Nákup technických prostriedkov, programových prostriedkov a služieb.
- Realizačná fáza projektu „Nasadenie“ bude prebiehať 5 mesiacov od ukončenia realizačnej fázy Implementácia a testovanie.

Každá realizačná fáza predstavuje samostatný fakturačný míľnik.

10. PRÍLOHY

Dokument neobsahuje prílohy.

Koniec dokumentu.