PRÍSTUP K PROJEKTU

(Verzia dokumentu v1.01/07_2021)

Identifikovanie požiadaviek **na technickú časť riešenia**

Identifikácia projektu

Povinná osoba	Národné centrum zdravotníckych informácií
Názov projektu	Budovanie kapacít a zvýšenia spôsobilosti pracoviska bezpečnostných operácii SOC NCZI
Zodpovedná osoba za projekt	Mgr. Silvia Strešková
Realizátor projektu	Národné centrum zdravotníckych informácií
Vlastník projektu	Mgr. Peter Lukáč, PhD., riaditeľ NCZI

Schvaľovanie dokumentu

Položka	**Meno a priezvisko**	**Organizácia**	**Pracovná pozícia**	**Dátum**	**Podpis** (alebo elektronický súhlas)
Vypracoval	Mgr. Silvia Strešková	Národné centrum zdravotníckych informácií	Projektový manažér	15.10.2023	

OBSAH

1. POPIS ZMIEN DOKUMENTU

1.1 História zmien

Verzia	Dátum	Zmeny	Meno
0.3	15.10.2023	Iniciálny dokument	Mgr. Silvia Strešková
0.4	10.11.2023	Upresnenie kapitol 4.1-4.8	Mgr. Silvia Strešková

2. ÚČEL DOKUMENTU

V súlade s **Vyhláškou 85/2020 Z.z. o riadení projektov** - je dokument **Projektový prístup** pre iniciačnú fázu určený na detailné technické rozpracovanie informácií o projekte.

2.1 Konvencie používané v dokumentoch – označovanie požiadaviek

ID	SKRATKA	POPIS
1.	API	Application programming interface
2.	BPMN	Business Process Model and Notation
3.	CSRÚ	Centrálna správa referenčných údajov
4.	DevOps	Je skrátený názov pre developer, security alebo aj automatizovaný devops ako súbor procesov medzi vývojom a prevádzkou, skratka z developer operations. Vysvetlenie detail viď https://en.wikipedia.org/wiki/DevOps
	DLP	Data Loss Prevention
5.	DMS	Document management system
	EDR/XDR	Endpoint detection and response / Extended detection and response
6.	EA model	UML model vedený v Enterprise Architect od Sparx, ktorý NCZI používa ako repository pre analytické modely
7.	ezdravie	Programové označenie Národného zdravotníckeho informačného systému
8.	eID	Elektronický občiansky preukaz s čipom
9.	EVS	Efektívna verejná správa
10.	ETL	Extract, Transform, Load
11.	EÚ	Európska únia
12.	EZKO	Elektronická zdravotná knižka občana
13.	GUI	Graphical user interface
14.	HW	Hardware
15.	HLD	High level dizajn – vysokoúrovňový dizajn napr architektúru, bezpečnosť
16.	IaaS	Infrastructure as a service
17.	IAM	Identity and Access Management
18.	IKT	Informačno-komunikačné technológie
19.	IS	Informačný systém
20.	IS PZS	Informačný systém poskytovateľov zdravotnej starostlivosti
21.	IS VS	Informačný systém verejnej správy
22.	ISZI	Informačný systém zdravotníckych indikátorov
23.	JRÚZ	Jednotná referenčná údajová základňa rezortu zdravotníctva.
24.	JRUZID	Jedinečný bezvýznamový identifikátor údaja v rámci jednotnej údajovej základne
25.	Komora	Stavovská organizácia v zdravotníctve definovaná zákonom č. 578/2004 Z. z.
26.	KPI	Key performance indicator – Kľúčové indikátory, prostredníctvom ktorých sa meria naplnenie cieľov projektu.
27.	KÚZZ	Konsolidovaná údajová základňa rezortu zdravotníctva
28.	KV	Kapitačný vzťah
29.	LLD	Low level dizajn – nízkoúrovňový dizajn napr. pre architektúru, bezpečnosť. Obsahuje detailné dizajny až na úrovní nastavení parametrov
30.	MDM	Mobile device management
31.	Mem cache	Časť JRUZ, ktorá slúži na získavanie referenčných záznamov z centrálneho repozitára údajov, na ktoré sú referencované všetky klinické záznamy v NZIS.

32.	MIRRI	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
33.	MV SR	Ministerstvo vnútra SR
34.	MZ SR	Ministerstvo zdravotníctva Slovenskej republiky
35.	NCZI	Národné centrum zdravotníckych informácií
36.	NFP	Nenávratný finančný príspevok
37.	NKIVS	Národná koncepcia informatizácie verejnej správy
38.	NZIS	Národný zdravotnícky informačný systém
39.	OOÚ	Ochrana osobných údajov
40.		
41.	PSK	Program Slovensko 2021 – 2027
42.	OVM	Orgán verejnej moci
43.	PaaS	Platform as a service
44.	PILOT	PILOT - Prevádzka riešenia na vybraných aktéroch na produkčnom prostredí.
45.	PoC	PoC - Implementovaný prototyp riešenia nasadený do produkčnej prevádzky a overený E2E testami minimálne s využitím mockov
46.	PPV	Pracovno-právny vzťah
47.	PR	Projektové riadenie
48.	PrZS	Prijímateľ zdravotnej starostlivosti
49.	PROD	PROD - Nasadené riešenie do produkčnej prevádzky, zaškolená prevádzka a nastavený proces zberu podnetov a riešenia chýb a zmien vrátane úprav kompletnej dokumentácie.
50.	PV	Poistný vzťah
51.	PZS	Poskytovateľ zdravotnej starostlivosti
52.	ROLLOUT	ROLLOUT - Postupné pripájanie ostatných aktérov na produkčnom prostredí.
54.	RFO	Register fyzických osôb
55.	RPO	Register právnických osôb
56.	RÚVZ	Regionálne úrady verejného zdravotníctva
57.	SDL metodika	Security development lifecycle – interná metodika pre postup implementácie vydaný NCZI.
58.	SFTP	SSH File Transfer Protocol
59.	SLA	Service level agreement
	SOAR	Security orchestration, automation and response
60.	SOAP	Simple Object Access Protocol
61.	SR	Slovenská republika
62.	ŠÚ SR	Štatistický úrad Slovenskej republiky
63.	ŠÚKL	Štátny ústav pre kontrolu liečiv
64.	ÚDZS	Úrad pre dohľad nad zdravotnou starostlivosťou
65.	VÚC	Vyšší územný celok alebo iný povoľovací orgán
66.	xservices	Spoločné služby pre všetky domény ezdravie. Ide o logickú skupinu služieb, ktoré sa využívajú vo všetkých procesoch zberu a zdieľania záznamov zdravotnej dokumentácie v ostatných doménach ezdravie.
67.	ZPr	Zdravotnícky pracovník vedený v príslušnej komore
68.	PR	Projektové riadenie
69.	VÚC	Vyšší územný celok alebo iný povoľovací orgán

3. POPIS NAVRHOVANÉHO RIEŠENIA

Projekt budovania kapacít a zvýšenia spôsobilosti pracoviska bezpečnostných operácii SOC NCZI je zameraný na dobudovanie infraštruktúry, posilnenie kybernetickej bezpečnosti NZIS a vybraných IS subjektov v zriaďovateľskej pôsobnosti MZ SR, zlepšenie procesov, komunikácie, zberu dát, analýzy, predchádzanie incidentom a zrýchlenie riešenia kybernetických bezpečnostných incidentov zvýšenie personálnej a znalostnej spôsobilosti pracoviska SOC a zabezpečenie primeraných pracovných podmienok pracoviska SOC.

Iniciatíva projektu vychádza z viacerých základných predpokladov, ktoré sú zároveň vzájomne previazané:

- Nárast rizika kybernetických útokov zameraných na subjekty poskytovateľov zdravotnej starostlivosti a kľúčové IS štátu po vypuknutí vojenského konfliktu na Ukrajine.
- Potreba posilnenia personálnych kapacít špecialistov interného tímu pre potreby vykonávania analýz a stabilizácia kľúčových členov a podporného tímu administrátorov jednotlivých technológii.
- Potreba zvýšenia visibility v monitorovaných IS a dobudovanie forenzného laboratória, laboratória dátových analýz, laboratórium malvér vyplývajúca.
- Ambícia získania kompetencie pre zriadenie a prevádzkovanie jednotky CSIRT pre rezort zdravotníctva.
- Potreba kontinuálneho vzdelávania a zvyšovania znalostného štandardu pracoviska SOC NCZI.
- Naplnenie zákonných a regulatórnych požiadaviek.

Cieľmi projektu sú zvýšenie spôsobilostí po technickej, procesnej a personálnej stránke, stabilizácia jadra tímu a naplnenie predpokladov cieľa vytvorenia a prevádzkovania rezortnej jednotky CSIRT.
Ciele budú naplnené nasledovnými aktivitami:

- Zefektívnenie procesov reakcie na bezpečnostné hrozby a zníženie potreby manuálnej intervencie pri riešení incidentov implementáciou nástroja SOAR.
- Zvýšenie visibility a kvality zdrojov logov implementáciou: EDR, DLP, MFA, Skener zraniteľnosti, SOAR, Dátová analýza, Forenzný lab, Malvér lab, Vybavenie pracoviska SOC, Mobile device MGMT MDM, WAF, Network EDR.

Implementácia vyššie uvedených technológie prispeje k rozšíreniu poskytovaných služieb SOC NCZI pre monitorované IS o proaktívne služby s rozšírením zberu a kvality bezpečnostne relevantných informácií ich evidencie triedenia, zrýchlenie identifikácie, analýzy a riešenie hrozieb, čím sa znižuje doba, počas ktorej je organizácia vystavená riziku. Integrácie implementovaných bezpečnostných nástrojov umožní centralizované riadenie a monitorovanie bezpečnostných operácií. Tieto platformy budú prispôsobené konkrétnym potrebám a prostrediam organizácie tak, aby zabezpečili optimálnu ochranu pred kybernetickými hrozbami.

Rozšírenie poskytovaných služieb bude zároveň podporené školeniami, vzdelávaním a systémom vlastných personálnych kapacít pre udržanie a stabilizáciu personálu a finančným krytím pre nábor nových špecialistov pod dobu trvania projektu. Ciele projektu korešpondujú s dlhodobou stratégiou rozvoja SOC NCZI, ktorá súvisí s postupným rozširovaním proaktívnych služieb a rozsahu monitorovaných IS subjektov rezortu zdravotníctva formou budovania bezpečnostného dohľadového centra s ambíciou rozvoja na rezortné pracovisko CSIRT. Rovnaké ciele sú súčasťou stratégiu NCZI a MZ SR. Naplnením cieľov projektu zabezpečíme plynule zvládnutie vyššej vyťaženosti tímu SOC NCZI pri prípadných útokoch a navýšení počtu monitorovaných subjektov.
Implementáciou riešenia sa dosiahne:

- Hĺbkový prehľad („visibility") o bezpečnosti IT prostredí, ktoré budú do Centrálneho bezpečnostného, logovacieho a vyhodnocovacieho nástroja pripojené, ktorý je nevyhnutný na včasné reakcie na kybernetické bezpečnostné ohrozenia;
- Automatizované výstrahy o incidentoch pri porušení bezpečnostných politík;
- Kontinuálny zber a možnosť analýzy sieťových tokov až do aplikačnej vrstvy OSI/ISO modelu;
- Možnosť forenznej analýzy sieťových tokov;
- Detekciu anomálií na úrovni tokov a rozpoznávanie známych hrozieb na základe DPI za pomoci detekčných signatúr.
- Identifikáciu porušenia interných bezpečnostných politík pomocou analýzy správania sa porovnaním s definovanou komunikačnou maticou, ako aj technikami na detekciu neštandardného správania sa v monitorovaných sieťach;
- Začlenia sa nové technické a technologické riešenia systému včasnej reakcie do infraštruktúry riadenia incidentov kybernetickej bezpečnosti;
- Implementuje rámec pravidelných hĺbkových bezpečnostných auditov, hodnotenia zraniteľnosti, ako aj penetračného testovania v celkovej architektúre kybernetickej bezpečnosti;
- Zvýši sa úroveň technologického bezpečnostného vybavenia zariadení kritickej infraštruktúry;
- Vypracuje sa katalóg hrozieb a metodika riadenia kybernetickej bezpečnosti;
- Vypracuje sa centralizovaný prístup k implementácii bezpečnostných záplat;
- V rámci prevencie sa posilní všeobecná úroveň kvality fyzickej a procesnej bezpečnosti kritickej infraštruktúry. To sa dosiahne zlepšením bezpečnosti procesu, rekonštrukciou a dobudovaním zabezpečených priestorov pre informačné systémy kritickej infraštruktúry.

Zvýšenie spôsobilosti Security Operation Center (SOC) je kľúčové pre zabezpečenie informačnej bezpečnosti a ochranu pred kybernetickými hrozbami pre NCZI ako centrálneho bodu zberu a spracovania zdravotníckych dát, ktorý predstavuje srdce celého procesu elektronizácie zdravotníctva. Realizáciou projektu dôjde k zvýšeniu spôsobilosti v nasledujúcich oblastiach:

- Rýchlejšia detekcia a reakcia na hrozby: Zlepšenie schopnosti identifikácie a reakcie na kybernetické hrozby v reálnom čase. To zahŕňa lepšiu analýzu logov, monitorovanie udalostí a upozornení, a automatizáciu procesov pre rýchlejšiu identifikáciu a potlačenie hrozieb.
- Rozšírená analýza hrozieb: Vytvorenie a zdokonalenie analytických schopnosti pre hĺbkovú analýzu kybernetických hrozieb implementáciou nástrojov na analýzu malvéru, rozpoznávanie správania útočníkov a predikcia budúcich hrozieb.
- Lepšie využitie technológií: Integrácia a efektívne využívanie nových technológii a nástrojov, ako sú umelá inteligencia, strojové učenie a automatizácia. To umožní rýchlejšie a presnejšie identifikovať hrozby a zároveň zníženie manuálnych úkonov.
- Zlepšenie spolupráce a komunikácia: Posilnenie spoluprácu medzi tímami v rámci organizácie, vrátane oddelení IT, prevádzky a vedenia, aby sa lepšie zdieľali informácie o hrozbách a koordinovali sa reakcie na incidenty.
- Odbornosť a školenia: Posilnenie spôsobilosti tímu SOC prostredníctvom odborných školení a certifikácií. Udržiavanie členov tímu oboznámených s najnovšími hrozbami a postupmi, a dobudovanie interného tímu náborom odborníkov na kybernetickú bezpečnosť.
- Kontinuálne zlepšovanie procesov: Pravidelné preskúmavanie a zlepšovanie pracovných postupov a procesov SOC na základe skúseností získaných počas detekcie a riešenia incidentov, implementáciou nástrojov a zvyšovaním znalostného štandardu členov tímu.
- Kontinuálna analýza úspešnosti: Monitorovanie úspešnosti SOC v detekcii, reakcii a prevencii kybernetických hrozieb pomocou merateľných ukazovateľov výkonu. Tieto údaje sa potom môžu použiť na ďalšie zlepšenie schopností pracoviska SOC.
- Pripravenosť na nové technológie a trendy: Pripravenosť na nové technológie, trendy a taktiky kybernetických útokov a prispôsobovať sa im v čo najkratšom čase.
- Zabezpečenie finančných a personálnych zdrojov: Zabezpečenie dostatočného financovania, personálnych a technických zdrojov pre efektívne fungovanie SOC.
- Sledovanie právnych a regulačných požiadaviek: Zabezpečiť, aby činnosti SOC boli v súlade s platnými právnymi a regulačnými požiadavkami týkajúcimi sa ochrany údajov a kybernetickej bezpečnosti.

Tieto aktivity pomôžu pracovisku SOC k vytvoreniu efektívneho a odolného systému na identifikáciu, monitorovanie a riešenie kybernetických hrozieb s cieľom ochrany organizácie pred potenciálnymi útokmi a položia základ budúceho rezortného pracoviska CSIRT.

4. ARCHITEKTÚRA RIEŠENIA PROJEKTU

Predmet projektu budovanie kapacít a zvýšenia spôsobilosti pracoviska bezpečnostných operácii SOC NCZI priamo reflektuje cieľ aktivít projektu a to posilnenie preventívnych opatrení, zvýšenie rýchlosti detekcie a riešenia incidentov s cieľom prispieť k vytvoreniu systému včasnej reakcie v oblasti kybernetickej bezpečnosti verejnej správy. Zmena biznis, aplikačnej a technologickej vrstvy architektúry nie je predmetom projektu. Rámcový popis riešenia je uvedený v Projektovom zámere.

4.1 Biznis vrstva

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.2 Aplikačná vrstva

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.2.1 Rozsah informačných systémov

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.2.2 Využívanie nadrezortných centrálnych blokov a podporných spoločných blokov (SaaS)

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.2.3 Prehľad plánovaného využívania podporných spoločných blokov (SaaS)

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.2.4 Prehľad plánovaných integrácií ISVS na nadrezortné centrálne bloky – spoločné moduly

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.2.5 Prehľad plánovaných integrácií ISVS na nadrezortné centrálne bloky - modul procesnej integrácie a integrácie údajov (IS CSRÚ)

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.2.6 Poskytovanie údajov z ISVS do IS CSRÚ

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.2.7 Konzumovanie údajov z IS CSRU

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.3 Dátova vrstva

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.3.1 Údaje v správe organizácie

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.3.2 Dátový rozsah projektu

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.3.3 Kvalita a čistenie údajov

4.3.3.1 Zhodnotenie objektov evidencie z pohľadu dátovej kvality

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.3.3.2 Role a predbežné personálne zabezpečenie pri riadení dátovej kvality

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.4 Referenčné údaje

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.4.1 Objekty evidencie z pohľadu procesu ich vyhlásenia za referenčné

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.4.2 Identifikácia údajov pre konzumovanie alebo poskytovanie údajov do/z CSRU

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.5 Otvorené údaje

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.6 Analytické údaje

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.7 Moje údaje

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.8 Prehľad jednotlivých kategórií údajov

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.9 Technologická vrstva

4.9.1 Prehľad technologického stavu

Súčasťou projektu je tiež doplnenie jednotlivých HW položiek pre potreby rozšírenie Bezpečnostnej vrstvy. Položky sú vylistované v zozname uvedenom v dokumente BC/CBA na karte HW a licencie. Doplnením jednotlivých položiek nedochádza k zmene architektúry technologickej vrstvy. Z dôvodu, že s jedná o projekt kybernetickej bezpečnosti detailný popis jednotlivých HW položiek na vyžiadanie.

4.9.2 Požiadavky na výkonnostné parametre, kapacitné požiadavky

Požiadavky na početnosť obstarávaných zariadení, príslušenstva a popis požadovaných vlastností jednotlivých položiek na vyžiadanie.

4.9.3 Návrh riešenia technologickej architektúry

Doplnením jednotlivých položiek nedochádza k zmene architektúry technologickej vrstvy. Požiadavky na obstarávané riešenie, príslušenstvo a popis požadovaných vlastností jednotlivých komponentov na vyžiadanie.

4.9.4 Využívanie služieb z katalógu služieb vládneho cloudu

Vládny cloud neposkytuje služby, ktoré sú predmetom projektu a tieto služby nie sú poskytované v rámci katalógu služieb vládneho cloudu.

4.9.5 Jazyková lokalizácia

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

4.10 Bezpečnostná architektúra

Návrh riešenia bezpečnostnej architektúry reflektuje cieľ projektu posilnenie preventívnych opatrení, zvýšenie rýchlosti detekcie a riešenia incidentov s cieľom prispieť k vytvoreniu systému včasnej reakcie v oblasti kybernetickej bezpečnosti verejnej správy. Predmetom projektu je implementácia riešenia, ktoré vychádza z analýzy súčasného stavu, bezpečnostnej a technickej architektúry prostredia NCZI, analýzy rizík a potreby naplnenia legislatívnych požiadaviek. Riešenie zabezpečí dodržanie minimálnej požadovanej bezpečnostnej úrovne

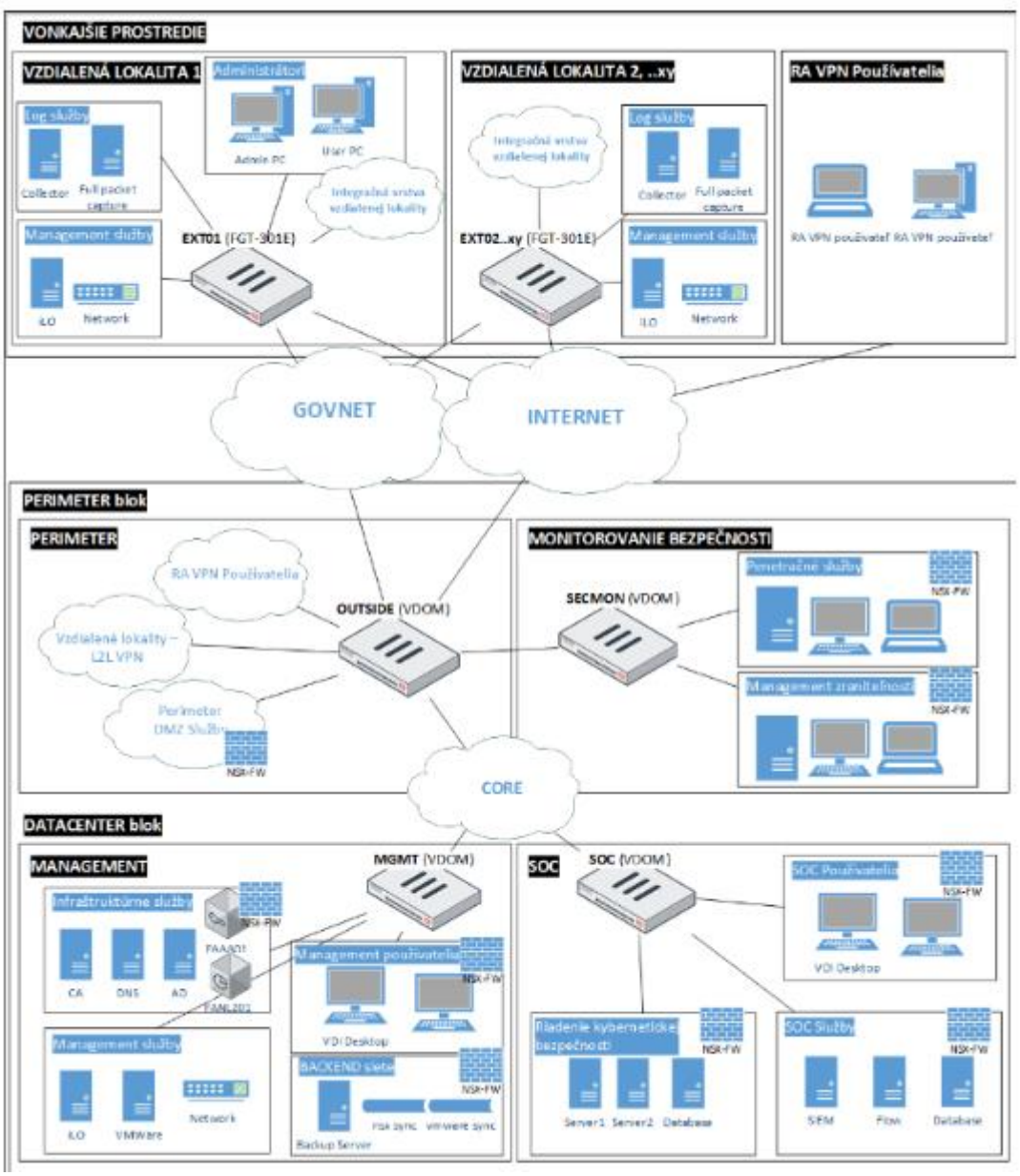
Za účelom zvýšenia úrovne zavedených postupov a opatrení týkajúcich sa kybernetickej a informačnej bezpečnosti (KIB) v NCZI je potrebné konsolidovať existujúcu bezpečnostnú architektúru a dobudovať security operation center implementáciou nových a inováciou existujúcich bezpečnostných nástrojov a procesov, a to najmä v nasledovných oblastiach:

- kybernetická ochrana a bezpečnostný monitoring a identifikácia bezpečnostných incidentov,
- riadenie bezpečnostných incidentov,
- ochrana proti externým hrozbám,
- ochrana dát, dátových prenosov a komunikácie,
- zvyšovanie bezpečnostného povedomia,
- implementácia bezpečnostných opatrení na zabezpečenie súladu so zákonom,

Služby a funkcie uvedené v tejto kapitole poskytujú z dôvodu, že sa jedná o projekt kybernetickej bezpečnosti len základné informácie a základný architektonický rámec riešenia, ktoré by malo byť implementované projektom. Budúce riešenie zabezpečenia informačnej a kybernetickej bezpečnosti sa bude skladať najmä z nasledovných funkcií:

- Kybernetická ochrana a detekcia škodlivých aktivít a bezpečnostných incidentov: Bezpečnostný monitoring IS, platforiem, aplikácií a používateľských činností a aktivít. Monitoring sietí, monitoring činností a aktivít privilegovaných používateľov. Analýza založená na big-data a machine learning algoritmoch.
- Riadenie bezpečnostných incidentov: Identifikácia a hlásenie bezpečnostných incidentov, registrácia, kategorizácia a klasifikácia bezpečnostných incidentov. Akceptácia bezpečnostných incidentov a určenie riešiteľov. Analýza a vyšetrovanie bezpečnostných incidentov a zber dôkazov. Riešenie bezpečnostných incidentov a obnova prevádzky, uzatvorenie bezpečnostných incidentov, vyhodnotenie bezpečnostných incidentov, zavedenie do KB DB, spätná väzba a poučenie sa z bezpečnostného incidentu.
- Zvýšenie ochrany pred útokmi z externého prostredia: Ochrana pred malware a ransomware, manažment bezpečnosti sietí, manažment bezpečnostných konfigurácií (implementácia systému pre jednotnú správu a deployment bezpečnostných politík a bezpečnostných konfigurácií).
- Ochrana dát, dátových prenosov a komunikácie: Bezpečnosť virtualizovaných prostredí, ochrana dát na úrovni databáz a dátových úložísk, ochrana dát na úrovni koncových zariadení. Riadenie prístupov (implementácia nástrojov IAM – riešenie IAM bude implemntované z DOP-OPII-16/2023, jeho prevádzka ani údržba nebude hradená z tohoto projektu). Proces bezpečnej výmeny informácií prostredníctvom EWS s vládnou jednotkou CSIRT, integráciou na JISKB, riadenie SW záplat (Patch management), manažment zraniteľností.
- Zvýšenie ochrany pred útokmi z externého prostredia: Ochrana pred malware a ransomware. Manažment bezpečnosti sietí, manažment bezpečnostných konfigurácií.

Schéma bezpečnostnej architektúry:



Popis jednotlivých blokov bezpečnostnej architektúry a požiadaviek na jednotlivé technológie:

FORENZNÝ LAB

Modul Forezný lab je zložený z HW a SW nástroja na Forenznú analýzu. Modul bude zabezpečovať digitálnu forenznú analýzu a správu elektronických dôkazov. Modul je určený pre zber, analýzy a správy dát a vizualizáciu ich vzájomných vzťahov. Taktiež implementuje nástroj na extrakciu a analýzu dát z mobilných zariadení a digitálnych médií, dešifrovanie týchto dát a generovanie reportov.

Funkcionality modulu Forenzný lab:

- Zber dát bez ich zmeny a poškodenia zo zariadení a úložných médií, ako sú pevné disky, pamäťové karty, USB kľúče a ďalšie.
- Hĺbková analýza digitálnych dát, vrátane vyhľadávania a identifikácie relevantných informácií.
- Správa a katalogizácia digitálnych dát a ich bezpečné uloženie a archivácia pre forenznú analýzu.
- Zabezpečenie integrity dát a dôkazov počas celého procesu forenzného vyšetrovania.
- Vizualizácia vzťahov medzi dátami a ich analýza vo forme grafov a diagramov pre potreby vyšetrovania komplexných prípadov.
- Vyhľadávanie a filtrovanie dát na základe rôznych kritérií, ako sú kľúčové slová, dátumy, typy súborov a ďalšie parametre.
- Podpora analýzy dát z rôznych operačných systémov, vrátane Windows, macOS a rôznych distribúcií Linuxu.
- Integrácia s ďalšími s ďalšími softvérovými nástrojmi a technológiami pre umožnenie rozšírenej funkcionality a efektívnej prácu s digitálnymi dátami.
- Logická a fyzická extrakcia systémových súborov alebo hesiel, či už zmazaných alebo chránených.
- Kompletná extrakcia existujúcich, skrytých a vymazaných údajov: SMS, MMS, kontakty, história hovorov, kalendár, e-mail, médiá, informácie o polohe (WiFi, navigačné aplikácie, geotagy) a ďalšie.

- Obchádzanie zámkou PIN/Pattern/Passcode z vybraných zariadení so systémom Android s akoukoľvek verziou.
- Fyzická extrakcia a pokročilé dekódovanie zo zariadení BlackBerry so systémom OS 4, 5, 6 a 7. Dešifrovanie v reálnom čase pre vybrané zariadenia.
- Analýza mobilných zariadení iOS chránené heslom, jailbreak-nuté, non-jailbreak-nuté, šifrované a nešifrované iOS zariadenia.

PENTEST LAB

Modul pre penetračné testovanie zabezpečí implementovanie testovania bezpečnosti webových aplikácií (Web Application Security Testing Tool), ktorý sa používa na identifikáciu a odstraňovanie bezpečnostných zraniteľností vo webových aplikáciách. Modul bude zabezpečovať automatizáciu penetračného testovania počas životného cyklu vývoja softvérových riešenie (SDLC).
Cieľom implemntácie pentest labu je automatizované skenovanie webových aplikácií s cieľom odhaliť rôzne druhy bezpečnostných zraniteľností, vrátane:
SQL Injection (SQLi): Vykonanie neoprávnených SQL dopyty na databázu.

- Cross-Site Scripting (XSS): Možnosti vkladania škodlivého kódu do webovej stránky, ktorý by mohli byť vykonané v prehliadači koncového používateľa.
- Cross-Site Request Forgery (CSRF): Vytváranie nežiaducich žiadosti v mene koncového používateľa.
- Bezpečnostné chyby v autentifikácii a autorizácii: Hľadá nedostatočnú autentifikáciu, autorizáciu a kontrolu prístupu.
- Nedostatočné ošetrenie vstupov, chyby vo vývoji a ďalšie.

Súčasťou pentest labu bude taktiež nástroj na simuláciu protivníka a operácii červeného tímu, ako spôsob hodnotenia bezpečnosti, ktoré replikujú taktiku a techniky pokročilého protivníka v sieti tzv. "red teaming" alebo "adversary simulation," pri ktorých bezpečnostné tímy, alebo iné organizácie testujú svoju vlastnú bezpečnosť pomocou nástrojov a taktík, ktoré by mohli použiť skutoční útočníci. Zatiaľ čo penetračné testy sa zameriavajú na neopravené zraniteľnosti a nesprávne konfigurácie, tieto posúdenia sú prínosom pre bezpečnostné operácie a reakciu na incidenty.
Hlavný účel nástroja:

- Umožňuje útočníkom pristupovať k cieľovým systémom a sieťam. Môže byť použitý na prekonanie obranných mechanizmov, ako sú firewally alebo antivirusové programy.
- Umožňuje útočníkom skákať cez viacero systémov a maskovať svoju prítomnosť, čím sa zvyšuje náročnosť detegovania ich aktivity.
- Zber informácii o cieľovom prostredí, vrátane informácií o systémových konfiguráciách a zraniteľnostiach.
- Exfiltrácia údajov z cieľového systému alebo siete.

MALVÉR LAB

Malvér lab implementuje sadu nástrojov:
Nástroj automatizovaného reverzného inžinierstva na analýzu softvérových aplikácií, zdrojového kódu a iných digitálnych entít za účelom pochopenia ich fungovania, identifikácie zraniteľností a iných bezpečnostných rizík.
Účel nástroja:

- Statická analýza zdrojového kódu analýzou binárnych súborov bez ich spúšťania pre potreby identifikácie škodlivých kódov, zraniteľností a ďalších aspektov bezpečnosti.
- Dynamická analýza zdrojového kódu sledovaním jeho správania v reálnom čase.
- Identifikácia zraniteľností a potenciálnych hrozieb v zdrojovom kóde.
- Detekcia malvéru a škodlivého softvéru v binárnych súboroch.
- Rozklad kódu pre potreby preverenia funkčnosti aplikácie, vrátane identifikácie funkcií, prenosov údajov.

Nástroj reverzného inžinierstva a analýzy binárneho kódu pre prácu s binárnym kódom a disassemblovaním programov.
Hlavnými účelom nástroja je:

- Možnosť prekladu binárneho kódu programu do ľudsky čitateľného assemblerového kódu pre účel analýzy funkčnosti a správania programu.
- Statická analýza disassemblovaného kódu a hľadanie rôznych typov chýb, bezpečnostných zraniteľností, malvéru a ďalších problémov.
- Použitie grafického používateľského rozhrania, ktoré umožňuje vizuálne prechádzať a analyzovať disassemblovaný kód a interagovať s ním.

Nástroj, ktorý umožňuje analýzu škodlivého softvéru a jeho správanie v izolovanom a bezpečnom prostredí.
Hlavný účel nástroja:

- Automatizácia procesu analýzy malvéru formou vykonávania testov a skenovaní nad škodlivým softvérom pre identifikáciu správania sa malvéru, zistenia rozsahu vykonávaných aktivít malvérom a rozsahu možných systémových zmien.
- Izolácia škodlivého softvéru od skutočného prostredia, čím sa minimalizuje riziko šírenia infekcie alebo poškodenia skúmaného systému.
- Sledovanie správania malvéru v kontrolovanom prostredí a analýza jeho interakcie s operačným systémom, súbormi a sieťovou komunikáciou. Tieto informácie pomáhajú bezpečnostným expertom pochopiť, aký je účel malvéru a aké sú jeho ciele.
- Generovanie záznamov z analýzy pre lepšie porozumenie hrozbám a vyvinutie stratégie na ich ochranu a odstránenie.
- Integrácia s inými bezpečnostnými nástrojmi a riešeniami na zlepšenie detekcie a reakcie na hrozby.
- Výsledkom použitia je lepšie porozumenie škodlivému softvéru, jeho charakteristikám a rizikám, ktoré predstavuje. To umožní organizácii zlepšiť svoju bezpečnosť a rýchlo reagovať na nové hrozby.

Nástroj na detekciu, monitorovanie a zbieranie informácií o kybernetických útočníkoch a hrozbách v informačných systémoch formou vytvárania falošného cieľa pre útočníkov.

Účel:

- Detekcia útokov zaznamenávaním všetkých aktivít útočníkov, ktorí sa pokúšajú zneužiť falošnú službu alebo systém. Týmto spôsobom umožňujú bezpečnostným tímom sledovať a analyzovať nové a existujúce kybernetické hrozby.
- Zber dôležitých informácií o technikách, nástrojoch a taktikách používaných útočníkmi. Tieto informácie môžu byť následne použité na zlepšenie bezpečnostných opatrení a obrany organizácie.
- Aktivity útočníkov na honeypotoch s cieľom odhaliť ich zraniteľnosti a slabiny umožňuje dozvedieť sa, aké časti jej siete alebo systému sú najviac ohrozené.
- Izolácia útočníkov a ich odstránenie z reálnej siete. Tým sa minimalizuje riziko pre skutočné systémy a umožňuje bezpečnostnému tímu čas na reakciu.

SOAR – MONITROING

Systém pre orchestráciu a automatizáciu bezpečnostných procesov (SOAR) s cieľom zefektívniť a urýchliť manuálne a časovo náročné úlohy v oblasti kybernetickej bezpečnosti. Jeho účelom je automatizovať opakujúce sa pracovné postupy v pracovisku Security Operations Center (SOC), orchestrovať rôzne bezpečnostné nástroje a zabezpečiť pokročilú, rýchlu, efektívnu a automatizovanú reakciu na bezpečnostné incidenty. SOAR systém umožňuje šetriť čas, finančné prostriedky a ľudské zdroje, zároveň posilňuje kybernetickú obranu organizácie. Obsahuje verejne dostupnú knižnicu s preddefinovanými pracovnými postupmi (workflows) a umožňuje organizáciám definovať vlastné pracovné postupy. Ďalšou výhodou je jednoduchá integrácia so SIEM (Security Information and Event Management) riešeniami, manažmentom zraniteľnosti a ticketovacími nástrojmi, čo zabezpečuje prehľadný reporting o spustených pracovných postupoch a celkový prehľad o kybernetických hrozbách a bezpečnostných incidentoch.

Požiadavky na riešenie:

- Automatizácia opakovaných pracovných postupov pracoviska SOC.
- Orchestrácia rôznych bezpečnostných a nebezpečnostných nástrojov.
- Pokročilejšia, zrýchlená, efektívnejšia a automatizovaná reakcia na incidenty.
- Šetrenie času, financií a ľudských zdrojov.
- Posilnenie kybernetickej obrany organizácie.
- Obsahuje verejne dostupnú knižnicu s preddefinovanými workflows.
- Umožňuje zadefinovať vlastné workflows.
- Jednoduchá integrácia so SIEM riešením, manažmentom zraniteľnosti, ticketovacím nástrojom.
- Prehľadný reporting spustených workflows.

SIEŤOVÝ FW (LOGSOURCE)

Zabezpečenie sieťového perimetra siete NCZI, z ktorej pristupujú správcovia k infromačným systémom NZIS.

INTEGRÁCIA NA THREAT INTELIGENCE PLATFORMU A JISKB

NCZI plánuje dobudovanie riešenia opensource servera MISP Malware Threat Intelligence ako platformy na zhromažďovanie, ukladanie, distribúciu a zdieľanie indikátorov kybernetickej bezpečnosti a hrozieb týkajúcich sa analýzy incidentov kybernetickej bezpečnosti a analýzy malvéru.

EDR

Cieľom implemntácie pokročilého riešenia Endpoint Detection and Response (EDR) je zabezpečiť bezpečnosť a ochranu všetkých koncových zariadení a serverov, v správe NCZI. Prioritou implemntácie modulu EDR je detekcia, monitorovanie a rýchla reakcia na kybernetické hrozby. Implemntáciou modulu EDR sa zabezpečí schopnosť identifikovať a zabrániť rôznym typom hrozieb, vrátane malvéru, ransomvéru a iných škodlivých aktivít, pričom toto riešenie podporuje tkz. „samoučiaci režim", ochranu pred neznámymi hrozbami a anti-ransomware ochranu. Riešenie umožní monitorovať všetky koncové zariadenia v reálnom čase, ponúknuť centralizovanú správu, vytvárať správy pre bezpečnostných administrátorov a definovať politiky pre jednotlivé skupiny administrátorov. EDR riešenie umožní rýchlu reakciu na incidenty, vrátane izolácie postihnutých zariadení, odstránenia hrozieb a obnovy systémov, a podporí threathunting s funkciou vizualizácie a minimálnou 30-dňovou retenciou dát. Cieľom je zabezpečiť bezpečnosť a ochranu všetkých koncových zariadení a serverov s dôrazom na detekciu, monitorovanie a rýchlu reakciu na kybernetické hrozby.

Minimálne požiadavky na riešenie EDR:

- Detekcia a prevencia hrozieb: Riešenie musí byť schopné identifikovať a zabrániť rôznym typom kybernetických hrozieb, vrátane malvéru, ransomvéru a iných škodlivých aktivít. Riešenie musí podporovať tzv. samoučiaci režim (machine learning), zero-day ochranu pred neznámymi hrozbami, anti-ramsoware ochranu (aktívne blokovanie neoprávneného šifrovania) a tiež skenovanie všetkých bežných súborov vrátane súborov typu obrázok.
- Monitorovanie a správa: Zákazník musí mať možnosť monitorovať všetky koncové zariadenia v reálnom čase a sledovať ich bezpečnostný stav. Riešenie musí ponúkať centralizovanú správu, vytváranie správ pre bezpečnostných administrátorov, umožňovať real-time správu klientov (serverov) a možnosti špecifických politík pre jednotlivé skupiny administrátorov.
- Rýchla reakcia na incidenty: EDR riešenie musí umožňovať rýchlu reakciu na detegované hrozby, vrátane izolácie postihnutých zariadení, odstránenia hrozieb a obnovy postihnutých systémov. Riešenie musí podporovať schopnosť threathuntingu (vrátane automatizovaného threathuntingu) s funkciou vizualizácie, pričom požadovaná data retention je minimálne 30 dní. Riešenie musí mať schopnosť analyzovať správanie sa administrátora servera a v prípade jeho neštandardného správania odmietnuť overenie.
- Kompatibilita a integrácia: Riešenie by malo byť kompatibilné s existujúcimi bezpečnostnými infraštruktúrami a mala by byť možnosť jeho integrovať s ďalšími bezpečnostnými nástrojmi, ako sú firewally, SIEM systémy atď.
- Výkonnosť a škálovateľnosť: EDR riešenie musí byť dostatočne výkonné a škálovateľné, aby dokázalo spravovať a chrániť veľký počet koncových zariadení bez degradácie výkonu. V rámci dodávky požadujeme licencie pre 1000 koncových zariadení s možnosťou škálovateľnosti až do 2000 používateľov.

- Aktualizácie a podpora: Dodávateľ musí poskytovať pravidelné aktualizácie bezpečnostných záplat a signatúr, tak ako aj technickú podporu v prípade problémov. Okrem licencie operačného systému musí riešenie obsahovať všetky licencie potrebné pre plnú funkcionalitu všetkých častí riešenia s platnosťou minimálne 12 mesiacov.
- Školenie a dokumentácia: Dodávateľ by mal poskytnúť školenie pre personál zákazníka a podrobnú dokumentáciu o používaní a konfigurácii riešenia.
- Dátová ochrana a súlad s reguláciami: Riešenie musí spĺňať všetky relevantné normy a regulácie v oblasti kybernetickej bezpečnosti a ochrany dát.

MDM

Modul pre správu a monitorovanie mobilných zariadení, ako sú mobilné telefóny a tablety, používané zamestnancami v pracovnom prostredí. Nástroj zabezpečí bezpečnosť firemných dát uložených na mobilných zariadeniach a zabráni neoprávnenému prístupu alebo úniku citlivých informácií. Implemntáciou nástroja sa vytvorí centralizovaný systém pre správu všetkých mobilných zariadení a aplikácií, vrátane možnosti vzdialenej konfigurácie a ich aktualizácie. Podpora BYOD (Bring Your Own Device) - umožní zamestnancom používať vlastné zariadenia v pracovnom prostredí, s dôrazom na oddelenie pracovných a osobných dát. Podpora COPE (corporate-owned, personally enabled) - umožní zamestnancom používať mobilné zariadenie vo vlastníctve zamestnávateľa pre pracovné aj osobné účely. Modul MDM Zabezpečí dodržiavanie nastavených pravidiel a politík spoločnosti a generovať správy o stave zariadení a aplikácií. Riešenie umožní registrovať a konfigurovať zariadenia, spravovať aplikácie a ich distribúciu, riadiť prístup a oprávnenia užívateľov, monitorovať a zaznamenávať aktivity, vzdialene spravovať a uzamknúť zariadenie v prípade jeho straty alebo krádeže.

Nástroj umožňujúci správu a monitorovanie mobilných zariadení, ako sú mobilné telefóny a tablety, ktoré sú používané zamestnancami v pracovnom prostredí.
Požiadavky:

- Zabezpečenie Dát: Zaistiť bezpečnosť firemných dát uložených na mobilných zariadeniach a zabrániť neoprávnenému prístupu alebo úniku citlivých informácií.
- Centralizovaná Správa: Vytvoriť centralizovaný systém pre správu všetkých mobilných zariadení a aplikácií, vrátane možnosti vzdialeného nastavenia a aktualizácií.
- Podpora BYOD: (Bring Your Own Device) - umožniť zamestnancom používať vlastné zariadenia v pracovnom prostredí, pričom zároveň zabezpečí oddelenie pracovných a osobných dát.
- Podpora COPE (corporate-owned, personally enabled) - možnosť zamestnancov používať mobilné zariadenie vo vlastníctve zamestnávateľa na pracovné aj súkromné účely.
- Súlad a Reporting: Vynucovanie nastavených pravidiel a politík spoločnosti a generovanie správ o stave zariadení a aplikácií.
- Registrácia a konfigurácia zariadenia.
- Správa aplikácií a ich distribúcia.
- Riadenie prístupu a práv užívateľov.
- Monitorovanie a logovanie aktivít.
- Vzdialená správa a blokovanie zariadenia v prípade straty alebo krádeže.
- Kompatibilita s rôznymi mobilnými operačnými systémami (iOS, Android, Windows).
- Silné zabezpečenie dát a možnosť vzdialeného vymazania.
- Intuitívne užívateľské rozhranie pre administrátorov.
- Integrácia na SIEM riešenia objednávateľa (IBM Qradar) v rozsahu zasielania bezpečnostne relevantných udalostí.

DLP

Technológia na identifikáciu, monitorovanie a ochranu citlivých dát a informácií pred ich stratou či odcudzením.
Požiadavky:

- On-premise riešenie.
- Automatizácia identifikácie, klasifikácie a monitorovania citlivých údajov.
- Zaistenie dodržiavania súladu s regulačnými nariadeniami (GDPR, ZoKB a ich vykonávajúce vyhlášky).
- funkcionality zachované i v offline móde, (ak koncová stanica nie je pripojená k firemnej sieti/ internetu).
- Integrácia na SIEM riešenia objednávateľa (IBM Qradar) v rozsahu zasielania bezpečnostne relevantných udalostí.
- Zaznamenávanie užívateľských akcií prevedených na Office 365 cloudu (OneDrive for Business, SharePoint Online, MS Teams) - základné súborové operácie ako sťahovanie a zdieľanie.
- Monitorovanie a vyhodnocovanie Office 365 emailové komunikácie (Exchange Online) pre všetkých užívateľov vrátane užívateľov pracujúcich z Outlook Web App, osobných alebo mobilných zariadení.
- Podpora POP3, IMAP, MAPI / Exchange protokolov vrátanie SSL šifrovania, podpora desktopových emailových klientov (Microsoft Outlook, Mozilla Thunderbird,…).
- Riešenie je schopné monitorovať emaily nezávisle od použitej aplikácie, podpora zaznamenávania súborov odoslaných cez web mailových klientov.
- Detailné informácie o práci so súbormi, ako prehľad užívateľov a aplikácií pracujúcich so súbormi, súborové operácie (otvorenie, premenovanie, kopírovanie, mazanie) a informácie o cestách (systémové, externé, webové, cloudové).
- Možnosť úplne blokovať užívateľské akcie, informatívna notifikácia užívateľa či samotné logovanie užívateľských akcií, ochrana citlivých dát, možnosť definície citlivých dát pomocou preddefinovaných slovníkov a algoritmov. Možnosť definície citlivých dát pomocou vlastných reťazcov či regulárnych výrazov. Možnosť importu vlastných slovníkov. Možnosť nastavenia počtu výskytov citlivých údajov. Dynamické reštrikcie nad súbormi a aplikáciami, pokiaľ je detegovaný citlivý obsah.
- Blokácia odoslania dát s citlivým obsahom mimo koncovú stanicu – správa bežných komunikačných kanálov: e-mail, web upload, externé zariadenie, IM (instant messaging) komunikačné nástroje, synchronizácia s cloudovými aplikáciami. Detekcia dát obsahujúcich citlivý obsah, uložených na koncovej stanici alebo na zdieľanom sieťovom disku. Možnosť integrácie s klasifikáciou tretích strán uložených v metadátach súborov.
- Reštrikcie pre USB zariadenia, pamäťové karty, Bluetooth zariadení alebo optické disky. Možnosť vynútenia režimu iba na čítanie u pripojených zariadení. Zaznamenávanie všetkých pripojených zariadení.
- Integrácia s MS Active Directory, Podpora pre MS SQL, Podpora operačných systémov Windows, Podpora serverových operačných systémov Windows Server 2008 R2, 2012 a 2016, podpora terminálových prostredí , centrálna administrátorská konzola, multitenantná administrácia v súlade s organizačným členením subjektov na úrovni OU domény, riadené

užívateľské práva k nastaveniam konzoly, k výsledným logom a administrácie riešenia a to vrátane lokálnych i doménových administrátorov.

Bezpečnostná architektúra je zároveň riešená v zmysle platnej legislatívy, nižšie vyberáme len niektoré platné zákony, predpisy a vyhlášky týkajúce sa kybernetickej a informačnej bezpečnosti:

- 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 nemá závislosti na iné projekty

6. ZDROJOVÉ KÓDY

Vzhľadom na charakter projektu – projekt z oblasti kybernetickej bezpečnosti je daná časť nerelevantná.

7. PREVÁDZKA A ÚDRŽBA

7.1 Prevádzkové požiadavky

Prevádzkové požiadavky budú pre navrhované riešenie rovnaké ako sú na existujúce informačné systémy.

Úrovne podpory používateľov:

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

- **L1 podpory IS** (Level 1, priamy kontakt zákazníka) – zabezpečuje Národné centrum zdravotníckych informácií
- **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).

Definícia:

- **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 predaných riešiteľom 1. úrovne podpory. Výstupom takejto kontroly môže byť potvrdenie, upresnenie, alebo prehodnotenie hlásenia v závislosti na potrebách Objednávateľa. Primárnym cieľom riešiteľov na úrovni Podpory L2 je dostať Hlásenie čo najskôr pod kontrolu a následne ho vyriešiť - s možnosťou eskalácie na vyššiu úroveň podpory – Podpora L3.

- **Podpora L3 (podpora 3. stupňa)** - Podpora 3. stupňa predstavuje najvyššiu úroveň podpory pre riešenie tých najobťažnejších Hlásení, vrátane prevádzania hĺbkových analýz a riešenie extrémnych prípadov.

Pre služby sú definované takéto SLA:

Služby pre zamestnancov úradu Po – Pia, 8:00 - 16:00 (8x5)

Riešenie incidentov – SLA parametre

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

Označenie naliehavosti incidentu:

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

možný dopad:

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

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

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

Vyžadované reakčné doby:

Označenie priority incidentu	Reakčná doba[1] od nahlásenia incidentu po začiatok riešenia incidentu	Doba konečného vyriešenia incidentu od nahlásenia incidentu (DKVI) [2]	*Spoľahlivosť*[3] *(počet incidentov za mesiac)*
1	0,5 hod.	4 hodín	*1*
2	1 hod.	12 hodín	*2*
3	1 hod.	24 hodín	*10*
4	1 hod.	Vyriešené a nasadené v rámci plánovaných releasov	

- (1) Reakčná doba je čas medzi nahlásením incidentu verejným obstarávateľom (vrátane užívateľov IS, ktorí nie sú v pracovnoprávnom vzťahu s verejným obstarávateľom) na helpdesk úrovne L3 a jeho prevzatím na riešenie.

- (2) DKVI znamená obnovenie štandardnej prevádzky - čas medzi nahlásením incidentu verejným obstarávateľom a vyriešením incidentu úspešným uchádzačom (do doby, kedy je funkčnosť prostredia znovu obnovená v plnom rozsahu). Doba konečného vyriešenia incidentu od nahlásenia incidentu verejným obstarávateľom (DKVI) sa počíta počas celého dňa. Do tejto doby sa nezarátava čas potrebný na nevyhnutnú súčinnosť verejného obstarávateľa, ak je potrebná pre vyriešenie incidentu. V prípade potreby je úspešný uchádzač oprávnený požadovať od verejného obstarávateľa schválenie riešenia incidentu.

- (3) Maximálny počet incidentov za kalendárny mesiac. Každá ďalšia chyba nad stanovený limit spoľahlivosti sa počíta ako začatý deň omeškania bez odstránenia vady alebo incidentu. Duplicitné alebo technicky súvisiace incidenty (zadané v rámci jedného pracovného dňa, počas pracovného času 8 hodín) sú považované ako jeden incident.

- (4) Incidenty nahlásené verejným obstarávateľom úspešnému uchádzačovi v rámci testovacieho prostredia
  a) Majú prioritu 3 a nižšiu
  b) Vzťahujú sa výhradne k dostupnosti testovacieho prostredia
  c) Za incident na testovacom prostredí sa nepovažuje incident vztiahnutý k práve testovanej funkcionalite.

Vyššie uvedené SLA parametre nebudú použité pre nasledovné služby:
- Služby systémovej podpory na požiadanie (nad paušál)
- Služby realizácie aplikačných zmien vyplývajúcich z legislatívnych a metodických zmien (nad paušál)

Pre tieto služby budú dohodnuté osobitné parametre dodávky.

7.2 Požadovaná dostupnosť IS:

Popis	Parameter	Poznámka
Prevádzkové hodiny	8 hodín	Po – Pia, 8:00 - 16:00
Servisné okno	14 hodín	od 17:00 hod. - do 7:00 hod. počas pracovných dní
	24 hodín	od 00:00 hod. - 23:59 hod. počas dní pracovného pokoja a štátnych sviatkov Servis a údržba sa bude realizovať mimo pracovného času.
Dostupnosť produkčného prostredia IS	97%	• 97% z 24/7/365 t.j. max ročný výpadok je 10,95 dňa. Maximálny mesačný výpadok je 21,9 hodiny. • Vždy sa za takúto dobu považuje čas od 0.00 hod. do 23.59 hod. počas pracovných dní v týždni. • Nedostupnosť IS sa počíta od nahlásenia incidentu Zákazníkom v čase dostupnosti podpory Poskytovateľa (t.j. nahlásenie incidentu na L3 v čase od 6:00 hod. - do 18:00 hod. počas pracovných dní). Do dostupnosti IS nie sú započítavané servisné okná a plánované odstávky IS. • V prípade nedodržania dostupnosti IS bude každý ďalší začatý pracovný deň nedostupnosti braný ako deň omeškania bez odstránenia vady alebo incidentu.

7.2.1 Dostupnosť (Availability)

Dostupnosť znamená, že dáta sú prístupné v okamihu jej potreby. Narušenie dostupnosti sa označuje ako nežiaduce zničenie (destruction) alebo nedostupnosť. Dostupnosť je zvyčajne vyjadrená ako percento času v danom období, obvykle za rok. V projekte sa uvažuje 97% dostupnosť znamená výpadok 10,95 dňa.

7.2.2 RTO (Recovery Time Objective)

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

7.2.3 RPO (Recovery Point Objective)

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

8. POŽIADAVKY NA PERSONÁL

Projekt sa bude riadiť v súlade s platnou legislatívou v oblasti riadenia projektov IT. Pre potreby riadenia projektu bude vytvorený riadiaci výbor projektu a budú menovaní členovia Riadiaceho výboru projektu (ďalej len „RV"), projektový manažér a členovia projektového tímu.

Najvyššou autoritou projektu je RV, ktorý tvorí:
a) **predseda** Riadiaceho výboru projektu,
b) **podpredseda** Riadiaceho výboru projektu,

c) **vlastník alebo vlastníci procesov NCZI** (biznis vlastník infraštruktúra) alebo nimi poverený zástupca alebo zástupcovia,
d) **vlastník alebo vlastníci procesov II. NCZI** (biznis vlastník II. architektúra) alebo nimi poverený zástupca alebo zástupcovia
e) **zástupcu kľúčových používateľov** (end user),
f) zástupca za Dodávateľa v zmysle Zmluvy o Dielo s Dodávateľom.
g) projektový manažér prijímateľa NFP.

Zloženie riadiaceho výboru:

ID	MENO A PRIEZVISKO	POZÍCIA	ORGANIZAČNÝ ÚTVAR	ROLA V PROJEKTE S UVEDENÍM HLASOVACIEHO PRÁVA
1.	Ing. Vladimír Daňo	TBD	TBD	Predseda RV (HP) – zástupca kľúčových používateľov
2.	Ing. Martin Laubert	TBD	TBD	Podpredseda RV (HP)
3.	Ing. Martin Puchalík	TBD	TBD	Zástupca vlastníkov procesov (HP)
4.	TBD	TBD	TBD	Zástupca vlastníkov procesov II. (HP)
5.	Ing. Martin Székely	TBD	TBD	Zástupcu kľúčových používateľov
6.	TBD	TBD	TBD	Zástupca Dodávateľa
7.	Mgr. Silvia Strešková	Projektový manažér	Odbor projektového riadenia	Projektový manažér prijímateľa

Zloženie projektového tímu:

- Povinné projektové role:
  - Projektový manažér,
  - Kľúčový používateľ,
  - Vlastník procesov,
  - IT analytik,
  - IT architekt,
  - Manažér kvality,
  - Manažér kybernetickej a informačnej bezpečnosti,
  - Špecialista pre bezpečnosť IT.
- Povinné plánované capacity:
  - Manažér SOC,
  - Špecialista bezpečnosti SOC,
  - Bezpečnostný analytik (úroveň L1, L2),
  - Incident Responder (úroveň L3),
  - Špecialista Threat intelligence,
  - Platform support engineer.
- Ďalšie projektové role:
  - Finančný manažér

ID	MENO A PRIEZVISKO	POZÍCIA	ORGANIZAČNÝ ÚTVAR	PROJEKTOVÁ ROLA
1.	Mgr. Silvia Strešková	Projektový manažér	Odbor projektového riadenia	Projektový manažér
2.	Ing. Vladimír Daňo	Riaditeľ odboru bezpečnostného monitoringu	Odbor bezpečnostného monitoringu	Kľúčový používateľ
3.	TBD	TBD	TBD	Vlastník procesov
4.	TBD	TBD	TBD	IT analytik
5.	TBD	TBD	TBD	IT architekt

6.	TBD	TBD	TBD	Manažér kvality
7.	TBD	TBD	TBD	Manažér kybernetickej a informačnej bezpečnosti
8.	TBD	TBD	TBD	Špecialista pre bezpečnosť IT
9.	TBD	TBD	TBD	Manažér SOC
10.	TBD	TBD	TBD	Špecialista bezpečnosti SOC
11.	TBD	TBD	TBD	Bezpečnostný analytik (úroveň L1, L2)
12.	TBD	TBD	TBD	Incident Responder (úroveň L3)
13.	TBD	TBD	TBD	Špecialista Threat intelligence
14.	TBD	TBD	TBD	Platform support engineer
15.	TBD	TBD	TBD	Finančný manažér

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

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

Ďalšie povinnosti členov RV, projektového manažéra a členov projektového tímu sú uvedené vo Vyhláške č. 85/2020 Z. z. a v doplňujúcich vzoroch a šablónach zverejnených na webovom sídle MIRRI SR.

Projektová rola:	**PROJEKTOVÝ MANAŽÉR**
Detailný popis ozsahu zodpovedností, povinností a kompetencií:	- zodpovedá za každodenné riadenie projektu v mene RV, za monitorovanie projektu, za plánovanie aktivít, za informovanie o projekte, atď., - zodpovedá za určenie pravidiel, spôsobov, metód a nástrojov riadenia projektu a získanie podpory RV pre riadenie, plánovanie a kontrolu projektu aefektívne využívanie projektových zdrojov (ľudských a finančných), - zodpovedá za splnenie všetkých legislatívnych požiadaviek (právne predpisy SR a EK), metodických požiadaviek súvisiacich s implementáciou projektu a formálnu administráciu projektu súvisiacu s riadením, organizovaním, finančným zúčtovaním, sledovaním čiastkových a celkových výsledkov (monitorovaním) a hodnotením výsledkov, - integrovane riadi prípravu a uskutočnenie projektu, nasadenie disponibilných prostriedkov, zabezpečuje koordináciu dodávateľov a zhotoviteľov jednotlivých výstupov projektu, zabezpečuje koordináciu partnerov, časový priebeh a kvalitu výstupov projektu, zmeny projektu a rieši konflikty s okolím projektu, - prijíma rozhodnutia a riadi projekt tak, aby sa splnili stanovené ciele projektu a aby projekt dodával dohodnuté produkty v dohodnutej kvalite, v čase a v rámci rozpočtu, - zodpovedá RV za plnenie cieľov projektu a celkový postup prác v projekte, - informuje RV o stave a priebehu projektu, predkladá návrhy na zlepšenie, - riadi strategické a projektové riziká, vrátane vývojových a rezervných plánov, - zodpovedá za identifikovanie kritických miest projektu a navrhovanie ciest k ich eliminácii, - aktívne komunikuje s dodávateľom, zástupcom dodávateľa a projektovým manažérom dodávateľa s cieľom zabezpečiť úspešné dodanie a nasadenie požadovaných projektových výstupov, - zabezpečuje kontrolu dodržiavania a plnenia míľnikov v zmysle zmluvy s dodávateľom, - zabezpečuje vecnú administráciu zúčtovania dodávateľských faktúr, - predkladá požiadavky dodávateľa na rokovanie RV, - zodpovedá za koordináciu azabezpečenie podkladov pre oddelenie komunikačné pre potreby medializácie projektu, - zodpovedá za informovanie zamestnancov a verejnosti o začatí a ukončení projektu v závislosti od jeho charakteru, - zodpovedá za zabezpečenie vypracovania, priebežnej aktualizácie a verzionovania manažérskej a špecializovanej dokumentácie a produktov, - pripravuje a predkladá stanovené dokumenty na schválenie RV, - navrhuje zaradiť projekt alebo jeho časť do režimu utajenia, - zabezpečuje permanentný dohľad a zvýšenú mieru kontroly a ochrany tokov informácií pri realizácii utajovaného projektu alebo utajovanej časti projektu, - zodpovedá za vypracovanie požiadaviek na zmenu, návrh ich prioritizácie a predkladanie zmenových požiadaviek na rokovanie RV, - zabezpečuje podanie žiadosti o rozpočtové opatrenie MF SR cez Rozpočtový informačný systém na projekt IT podľa potreby, - zodpovedá za riadenie zmeny a prípadné požadované riadenie konfigurácií,

	- navrhuje členov projektového tímu po dohode s líniovým vedúcim a tímovým manažérom a tiež navrhuje rozsah ich zodpovedností a činností, - organizuje, riadi, motivuje projektový tím a deleguje úlohy členom projektového tímu, - hodnotí členov projektového tímu, - udeľuje pokyny na výkon činností projektovej kancelárie, - podľa potreby deleguje svoje povinnosti a práva na tímových manažérov a koordinuje ich činnosť, - plní úlohy tímového manažéra (vedúceho projektového tímu), ak takáto rola v projekte nie je obsadená – viď činnosť projektovej role „Tímový manažér", - monitoruje výkonnosť projektu, to znamená, že sleduje pokrok vo vybraných ukazovateľoch (KPI) projektu a predkladá ho na schválenie RV, - zabezpečuje evidenciu v informačných systémoch pre štandardizované procesy programové a projektového riadenia, napr. IT monitorovací systém pre európske štrukturálne a investičné fondy, - zodpovedá za publikovanie RV schválených projektových výstupov v MetaIS chronologicky, z každej fázy životného cyklu projektu, - zodpovedá za publikovanie zápisov RV v MetaIS, - počas celej doby realizácie projektu štandardne zabezpečuje nasledovné prierezové činnosti: 1. kontinuálne zdôvodňovanie projektu, ktoré zahŕňa posúdenie, či je projekt požadovaný a dosiahnuteľný, potrebné na rozhodovanie o pokračovaní vynakladania prostriedkov počas všetkých fáz projektu, vypracované aspoň po ukončení každej fázy projektu, 2. plánovanie a operatívne riadenie dodávania projektových produktov, 3. riadenie rizík a závislostí, ktoré zahŕňa identifikáciu, hodnotenie a riadenie rizík, závislostí a hrozieb na úspešnú realizáciu projektu, - zabezpečuje dodržiavanie legislatívno-metodických zásad pre riadenie projektov, - zodpovedá za formálnu administráciu projektu, riadenie centrálneho úložiska projektovej dokumentácie FS, správu a archiváciu projektovej dokumentácie, - sleduje dodržiavanie interných riadiacich aktov.

Projektová rola:	**MANAŽÉR KVALITY**
Stručný popis:	- zodpovedá za úvodné nastavenie pravidiel riadenia kvality a za následné dodržiavanie a kontrolu kvality, - kontroluje, či sa riadenie a proces zabezpečenia kvality vykonáva správnym spôsobom, v správnom čase a správnymi osobami, - počas celej doby realizácie projektu zabezpečuje riadenie kvality projektových výstupov a zhodu projektových výstupov s požiadavkami definovaním merateľných výkonnostných parametrov na vytváranie, overovanie projektových produktov, definovanie akceptačných kritérií, ktoré sú vhodné na požadovaný účel, - počas celej doby realizácie projektu zodpovedá za priebežné vyžadovanie, hodnotenie a kontrolu kvality (vecnej aj formálnej), za plánovanie, zabezpečovanie, kontrolu, operatívne riadenie, zlepšovanie a vyhodnocovanie kvality projektu, - aktívne sa zúčastňuje stretnutí projektového tímu aspolupracuje na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Prílohou č.1 tejto smernice, - plní pokyny PM a dohody zo stretnutí projektového tímu, - spolupracuje s PM, - zodpovedá sa PM, - informuje PM o stave plnenia úloh, o zisteniach a o rizikách, - sleduje a hodnotí kvalitatívne ukazovatele projektových výstupov, - zabezpečuje zhodnotenie kvality projektu zamerané na výstupy iniciačnej a realizačnej fázy projektu formou auditu na mieste, ktorého výsledky spracuje v produkte M-04 Audit kvality.
Detailný popis ozsahu zodpovedností, povinností a kompetencií	• 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 – odôvodenie projektu s katalógom funkčných, nefunkčných a technických požiadaviek, • kontrolu kvality 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, • 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, • 15. kontrolu plnenia finančného plánu projektu,

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

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

Projektová rola:	**MANAŽÉR KYBERNETICKEJ A INFORMAČNEJ BEZPEČNOSTI („KIB“)**
Stručný popis:	- má neobmedzený aktívny prístup ku všetkým projektovým dokumentom, nástrojom a výstupom projektu, v ktorých sa opisuje predmet projektu z hľadiska jeho architektúry, funkcií, procesov, manažmentu informačnej bezpečnosti a spôsobov spracúvania dát, ako aj dát samotných, - má sprístupnené všetky informácie o bezpečnostných opatreniach zavádzaných projektom v zmysle § 20 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v

	znení neskorších predpisov a v zmysle ustanovení zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, - zodpovedá za posúdenie možných alternatív realizácie projektu za oblasť IB a KB, - zodpovedá za posúdenie požiadaviek agendy IB a KB na rozhrania a spoločné komponenty, na integrácie a procesy konverzie a migrácie, identifikácia nesúladu a návrh riešenia, - poskytuje konzultácie a súčinnosť pre problematiku IB a KB, - poskytuje konzultácie pri tvorbe šablón a vzorov dokumentácie pre oblasť IB a KB, - poskytuje konzultácie a vykonáva kontrolnú činnosť zameranú na obsah a komplexnosť dokumentácie z hľadiska IB a KB, - dohliada na zosúladenie projektu s princípmi definovanými v interných riadiacich aktoch FS a dokumentoch týkajúcich sa bezpečnosti FS, - zabezpečuje získavanie a spracovanie informácií nutných pre plnenie úloh v oblasti IB a KB, - aktívne sa zúčastňuje stretnutí projektového tímu a spolupracuje na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Prílohou č.1 tejto smernice, - plní pokyny PM a dohody zo stretnutí projektového tímu.
Detailný popis ozsahu zodpovedností, povinností a kompetencií	- zodpovedá za špecifikovanie: • štandardov, princípov a stratégií v oblasti informačnej bezpečnosti („IB“) akybernetickej bezpečnosti („KB“) a ich dodržiavanie, • funkčných, nefunkčných a technických požiadaviek na IB a KB a za ich analýzu, • požiadaviek na IB a KB, kontroluje ich implementáciu v realizovanom projekte, • požiadaviek na bezpečnosť vývojového, testovacieho a produkčného prostredia, • požiadaviek na bezpečnosť v rámci bezpečnostnej vrstvy, • požiadaviek na školenia pre oblasť IB a KB, • požiadaviek na bezpečnostnú architektúru riešenia a technickú infraštruktúru pre oblasť IB a KB, • požiadaviek na dostupnosť, zálohovanie, archiváciu a obnovu IS vzťahujúce sa na IB a KB, • požiadaviek na IB a KB, bezpečnostný projekt a riadenie prístupu, • požiadaviek na opis vývojového, testovacieho a produkčného prostredia za oblasť IB a KB, • požiadaviek na testovanie z hľadiska IB a KB, realizáciu kontroly zapracovania a retestu, • požiadaviek na obsah dokumentácie v zmysle legislatívnych požiadaviek pre oblasť IB a KB, ako aj v zmysle "best practies", • požiadavieknadodaniepotrebnejdokumentáciesúvisiacejsIBaKBkontrolujeichimplementáciu v realizovanom projekte, • požiadaviek a konzultácie pri návrhu riešenia za agendu IB a KB v rámci procesu „Mapovanie a analýza technických požiadaviek - detailný návrh riešenia (DNR)“, • požiadavieknabezpečnosť ITaKB vrámci procesu "akceptácie, odovzdania a správy zdrojových kódov“, • akceptačných kritérií za oblasť IB a KB, • pravidiel pre publicitu a informovanosť s ohľadom na IB a KB, • podmienok na testovanie, reviduje výsledky a výstupy z testovania za oblasť IB a KB, • požiadaviek na bezpečnostný projekt pre oblasť IB a KB, - zodpovedá za realizáciu kontroly: • zameranej na naplnenie požiadaviek definovaných v bezpečnostnom projekte za oblasť IB a KB, • zameranú na správnosť nastavení a konfigurácii bezpečnosti jednotlivých prostredí, • zameranú na realizáciu procesu posudzovania a komplexnosti bezpečnostných rizík, bezpečnosť a kompletný popis rozhraní, správnu identifikácia závislostí, • naplnenia definovaných požiadaviek pre oblasť IB a KB, • zameranú na implementovaný proces v priamom súvise s IB a KB, • súladu s platnou legislatívou v oblasti IB a KB (obsahuje aj kontrolu legislatívnych požiadaviek), • zameranú na zabezpečenie procesu, interfejsov, integrácii, kompletného popisu rozhraní a spoločných komponentov a posúdenia z pohľadu bezpečnosti,

Projektová rola:	**ČLEN PROJEKTOVÉHO TÍMU**
Stručný popis:	- vykonáva odbornú prácu v projekte a poskytuje odborné stanoviská a konzultácie za príslušnú oblasť, - aktívne sa zúčastňuje odborných stre **Cieľom aktivít projektu je vytvoriť prostredie na národnej úrovni v ktorom bude možné čo najefektívnejšie zvyšovať úroveň kybernetickej bezpečnosti pre samosprávy SR a občanov SR využívajúcich elektronické služby samospráv.** tnutí tímu, ako aj konzultácií, - zabezpečuje vypracovanie, priebežnú aktualizáciu a verzionovanie manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Prílohou č.1 tejto smernice v súčinnosti a podľa pokynov tímového manažéra a PM, - plní úlohy uložené tímovým manažérom a PM v požadovanej kvalite a v stanovených termínoch, - plní dohody zo stretnutí projektového tímu, - odpočtuje plnenie úloh tímovému manažérovi a PM,

	- predkladá námety, podnety, požiadavky a upozorňuje na problémy a riziká súvisiace s projektom tímovému manažérovi a PM, - spolupracuje s projektovým tímom na strane dodávateľa, - zodpovedá za splnenie všetkých legislatívnych požiadaviek (právne predpisy SR a EK) a metodických a administratívnych požiadaviek súvisiacich s implementáciou projektu.

9. IMPLEMENTÁCIA A PREBERANIE VÝSTUPOV PROJEKTU

Projekt bude v zmysle Vyhlášky 85/20202 Zz o projektovom riadení realizovaný metódou waterfall. V zmysle vyhlášky 85/2020 Zz o projektovom riadení je možné pristupovať k realizácii projektu prostredníctvom čiastkových plnení, t.j. inkrementov. V projekte je definovaný jeden inkrement na obdobie hlavných aktivít.

10. PRÍLOHY

Koniec dokumentu.