projekt_2930_Pristup_k_projektu_ramcovy

PRÍSTUP K PROJEKTU

Vzor pre manažérsky výstup I-03

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

Povinná osoba	Katolícka univerzita v Ružomberku
Názov projektu	*Zvýšenie úrovne kybernetickej bezpečnosti na Katolíckej univerzite v Ružomberku*
Zodpovedná osoba za projekt	Ing. František HORVÁT, PhD.
Realizátor projektu	Katolícka univerzita v Ružomberku
Vlastník projektu	Katolícka univerzita v Ružomberku

Schvaľovanie dokumentu

Položka	Meno a priezvisko	Organizácia	Pracovná pozícia	Dátum	Podpis (alebo elektronický súhlas)
Vypracoval	Ing. František HORVÁT, PhD.	KU Ružomberok	Prorektor pre rozvoj, informatizáciu a inovácie	10.7.2024	

1. História dokumentu

Verzia	Dátum	Zmeny	Meno
0.1	5.6.2024	*Pracovný návrh*	Ing. František HORVÁT, PhD.
1.0	10.7.2024	*Zapracovanie súladu s vyhláškou č. 401/2023 Z. z., finálna verzia v súlade so ŽoNFP*	Ing. František HORVÁT, PhD.

2. Účel dokumentu

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

Dokument Prístup k projektu v zmysle vyššie uvedenej vyhlášky a požiadaviek výzvy: PSK-MIRRI-614-2024-DV-EFRR (Podpora v oblasti kybernetickej a informačnej bezpečnosti na regionálnej úrovni – verejné a štátne vysoké školy) 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.

V zmysle usmernenia MIRRI SR sa v projektovej dokumentácii (ani v žiadosti) nešpecifikujú detailne konkrétne riziká a dopady a nezverejňuje sa podrobná dokumentácia toho, kde sú najväčšie riziká IT systémov a uvádzajú sa iba oblasti identifikovaných rizík a dopadov. Zároveň je možné manažérske produkty napísať všeobecne.

2.1 Použité skratky a pojmy

Z hľadiska formálneho sú použité skratky a pojmy rámci celého dokumentu definované priebežne, štandardne pri prvom použití v zátvorke označením „ďalej len“.

2.2 Konvencie pre typy požiadaviek (príklady)

V rámci projektu budú definované tri základné typy požiadaviek:

Funkčné (používateľské) požiadavky majú nasledovnú konvenciu:

IDxx

ID – funkčná požiadavka xx – číslo požiadavky

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

IDxx

ID – nefukčná požiadavka (NFR) xx – číslo požiadavky

Technické požiadavky majú nasledovnú konvenciu:

IDxx

ID – technická požiadavka xx – číslo požiadavky

3. Popis navrhovaného riešenia

Navrhované riešenie vychádza z aktuálneho stavu kybernetickej bezpečnosti na Katolíckej univerzite v Ružomberku (ďalej len „KURK“). KURK si uvedomuje, že v zmysle požiadaviek zákona o kybernetickej bezpečnosti a zavedených opatrení v zmysle vyhlášky 362/2018 Z.z. (ďalej len ZoKB), ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška 362/2018 Z.z.) spĺňa len čiastočnú úroveň ustanovených požiadaviek.

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

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

ID	Názov cieľa	Názov strategického cieľa*	Spôsob realizácie strategického cieľa
1	Vytvorenie katalógu informačných aktív a realizovaním analýzy rizík na identifikovaných aktívach Cieľ realizovaný v zmysle oprávnených podaktivít: - Riadenie rizík	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Vypracovanie a aktualizácia stratégie kybernetickej bezpečnosti a bezpečnostnej dokumentácie s prihliadnutím na štruktúru bezpečnostnej dokumentácie podľa prílohy č.1 vyhlášky 362/2018 Z.z. Vypracovaná dokumentácia bude pokrývať všetky požadované oblasti požadovanej legislatívy. Vypracovaný bude katalóg informačných aktív s určením vlastníkov a administrátorov jednotlivých aktív. Vypracovaný bude katalóg hrozieb a rizík a na základe týchto katalógov bude vypracovaná analýza rizík pre jednotlivé aktíva. Kompletná identifikácia informačných aktív organizácie, vytvorenie katalógu aktív s určením vlastníkov a administrátorov jednotlivých aktív. Vypracovanie zoznamu hrozieb a ohodnotenie dopadov na aktíva z pohľadu triády CIA. Vypracovanie smernice pre riadenie rizík, podľa ktorej bude vykonávaná analýza rizík informačných systémov univerzity.
2	Zabezpečenie organizácie kybernetickej a informačnej bezpečnosti Cieľ realizovaný v zmysle oprávnených podaktivít: - Organizácia kybernetickej a informačnej bezpečnosti - Personálna bezpečnosť - Riadenie prístupov - Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami - Bezpečnosť pri prevádzke informačných systémov a sietí - Hodnotenie zraniteľností a bezpečnostné aktualizácie - Ochrana proti škodlivému kódu - Sieťová a komunikačná bezpečnosť - Zaznamenávanie udalostí a monitorovanie	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Vytvorenie, resp. aktualizácia kompletnej bezpečnostnej dokumentácie podľa požiadaviek ZoKB Prílohy č. 1 k vyhláške č. 362/2018 Z. z. Vypracovanie bezpečnostnej politiky pre univerzitu ohľadom riadenia, kontroly a vyhodnocovania stavu kybernetickej bezpečnosti na univerzite. Jedná sa o dokumentáciu, ktorá nie je zahrnutá v jednotlivých kapitolách - stratégia, bezpečnostná politika,... Vypracovanie postupov pri nástupe a odchode zamestnanca primárne z pohľadu prideľovania a odoberania prístupov do informačných systémov univerzity. Vypracovanie smernice pre koncových užívateľov a administrátorov, podľa ktorej sa bude riadiť bezpečnosť pri narábaní s pridelenými výpočtovými prostriedkami a pri prístupe do informačných systémov univerzity. Vypracovanie smernice pre riadenie prideľovania bezpečnostných rolí a úrovní prístupov pre interných a externých zamestnancov z dôvodu umožnenia prístupu k informačným systémom univerzity. Určenie a revízia dodávateľských zmlúv s tretími stranami, ktoré majú vplyv na poskytovanie kritických systémov organizácie. Návrh zmien v zmluvách týkajúcich sa oblasti kybernetickej bezpečnosti. Vypracovanie návrhu dodatku k zmluve s treťou stranou, ktorý bude pokrývať požiadavky ZoKB, ktoré sa týkajú dodávateľských vzťahov.

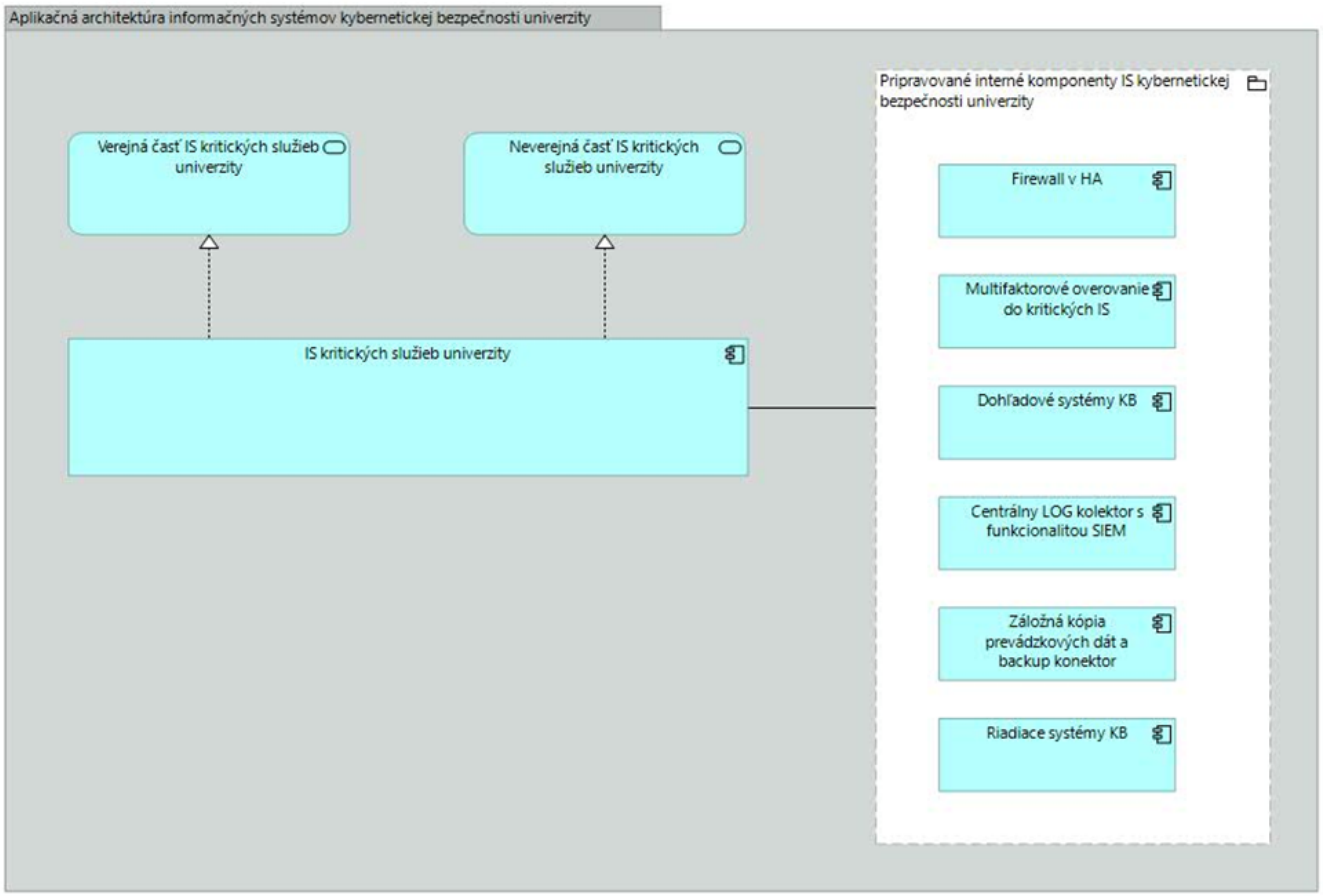
	- Fyzická bezpečnosť a bezpečnosť prostredia - Riešenie kybernetických bezpečnostných incidentov - Kryptografické opatrenia - Kontinuita prevádzky - Audit a kontrolné činnosti		Vypracovanie smernice pre administrátorov, podľa ktorej sa budú riadiť pri správe interných systémov univerzity. Vypracovanie postupov pre aplikovanie zmien v informačných systémoch univerzity a smerníc pre zaznamenávanie prevádzkových a bezpečnostných nastavení systémov. Vypracovanie interného riadiaceho dokumentu upravujúceho proces riadenia implementácie bezpečnostných aktualizácií a záplat. Vypracovanie smernice na určenie zodpovednosti používateľov. Vypracovanie interného riadiaceho dokumentu upravujúceho pravidlá sieťovej a komunikačnej bezpečnosti Vypracovanie dokumentácie spôsobu monitorovania a fungovania centrálneho log manažment systému a centrálneho nástroja na bezpečnostné monitorovanie a zadefinovanie spôsobu evidencie prevádzkových záznamov, ich vyhodnocovania, spôsobu hlásenia podozrivej aktivity, zodpovednej osoby a ďalších povinností. Vypracovanie smernice pre fyzickú a objektovú bezpečnosť, ktorá bude definovať požiadavky na zabezpečené priestory a na prístup do týchto priestorov. Vypracovanie štandardov a postupov riešenia kybernetických bezpečnostných incidentov, vrátane definovania zodpovedností zamestnancov a ďalších povinností, vypracovanie plánov a spôsobov riešenia kybernetických bezpečnostných incidentov. Vypracovanie smernice pre kryptografické opatrenia, ktorá bude definovať používanie a uchovávanie informácií týkajúcich sa použitých prístupových hesiel a kľúčov, bezpečnostných cetifikátov a ostatných bezpečnostných prvkov. Vypracovanie smernice pre posudzovanie bezpečnosti informačných systémov verejnej správy a ich vyhodnocovania.
3	Zvýšenie sieťovej a komunikačnej bezpečnosti nasadením a implementáciou NGFW do siete Cieľ realizovaný v zmysle oprávnených podaktivít: - Sieťová a komunikačná bezpečnosť	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Implementácia a konfigurácia perimetrového firewallu za účelom zabezpečenia bezpečného oddelenia internej siete a internetu. Úlohou tohto firewallu bude aj riešiť bezpečný prestup medzi segmentami siete a taktiež bude zabezpečovať bezpečný vzdialený prístup do siete na základe VPN spojení s overovaním pomocou dvojfaktorovej autentizácie. Zariadenia budú poskytovať pokročilé funkcie ako hĺbková inšpekcia sieťovej prevádzky, detekcia a prevencia hrozieb.
4	Implementácia centrálneho log manažment systému pre zber a ukladanie logov zo systémov univerzity s možnosťou korelácie incidentov a eventov a vytvárania alertov Cieľ realizovaný v zmysle oprávnených podaktivít: - Zaznamenávanie udalostí a monitorovanie	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Zaobstaranie, implementácia a konfigurácia samostatného centrálneho logovacieho systému, ktorý bude bezpečným spôsobom zbierať, vyhodnocovať, vizualizovať a ukladať systémové logy zo všetkých dôležitých systémov organizácie.

5	Implementácia systému na sledovanie prevádzkových parametrov a kapacít využívaných systémových prostriedkov. Cieľ realizovaný v zmysle oprávnených podaktivít: - Sie Zaznamenávanie udalostí a monitorovanie ťová a komunikačná bezpečnosť	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Implementácia dohľadového systému na sledovanie prevádzkových parametrov siete a systémov. Ide primárne o sledovanie dostupnosti jednotlivých zariadení, systémov a služieb a o sledovanie vyťaženosti systémov a služieb na týchto systémoch. Vytvorenie a zadefinovanie hraničných parametrov tak, že pri ich prekročení budú administrátori notifikovaní o vzniknutí tejto udalosti.
6	Zvýšenie bezpečnosti pri prevádzke informačných systémov a sietí dobudovaním záložných dátových kapacít Cieľ realizovaný v zmysle oprávnených podaktivít: - Bezpečnosť pri prevádzke informačných systémov a sietí - Fyzická bezpečnosť a bezpečnosť prostredia	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Implementácia zabezpečeného systému zálohovania vo fyzicky oddelenej budove za účelom zabezpečenia kópie dôležitých systémov a dát v prípade zlyhania alebo zničenia primárnej serverovne. Systém zálohovania by mal mať ochranu pred zmazaním a prepísaním uložených dát a mal by uchovávať zálohy v šifrovanej podobe. Zaobstaranie licencií potrebných pre úspešné prevádzkovanie bezpečného zálohovania dôležitých systémov a dát. Implementácia archivačného konektora pre existujúce systémy ISVS Zabezpečenie kontinuity prevádzky informačných systémov univerzity v prípade zlyhania alebo inej príčiny. Implementácia a konfigurácia zálohovacieho a archivačného konektora pre existujúce systémy ISVS eSPIS - konektory pre zálohovanie a archiváciu Obstaranie a implementácia dátového úložiska pre potreby zálohy prevádzkových dát a archivačnej kópie pomocou obstarania záložných kapacít pre ukladanie prevádzkových dát, umiestnené v zabezpečenom priestore bezpečne vzdialenom zálohovanému zabezpečenému priestoru. Tento bod bude splnený dodávkou HW zariadení na rozšírenie aktuálne prevádzkovaného diskového poľa NetApp. Potrebným navýšením diskových kapacít pre ukladanie zálohy prevádzkových dát a pomocou existujúceho softvéru na zálohovanie. - Dodávka hardvéru na rozšírenie aktuálneho diskového poľa. - Realizácia inštalačných a konfiguračných služieb, ktoré zabezpečia možnosť ukladania zálohy prevádzkových dát, vrátane testovacej obnovy dát
7	Vypracovanie plánov kontinuíty a ich otestovanie Cieľ realizovaný v zmysle oprávnených podaktivít: - Kontinuita prevádzky	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Vypracovanie stratégie a krízových plánov pre tri kritické systémy univerzity v prevádzke na základe analýzy vplyvov kybernetického bezpečnostného incidentu na základnú službu. Vypracovanie dekompozície dôležitých služieb a vypracovanie BIA pre tieto služby, resp. systémy. Vypracovanie plánov kontinuity prevádzky a ich prvotné otestovanie v reálnom prostredí organizácie a zapracovanie nedostatkov z výsledkov testovania.
8	Nezávislý audit kybernetickej bezpečnosti Cieľ realizovaný v zmysle oprávnených podaktivít: - Audit a kontrolné činnosti	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Po skončení implementácie všetkých opatrení obsiahnutých v projekte bude vykonaný nezávislý audit kybernetickej bezpečnosti.

4. Architektúra riešenia projektu

Architektúra celého riešenia je v zmysle usmernenia MIRRI SR rámcovaná tak, aby bolo z projektu zrejmé, ktoré komponenty v rámci realizácie projektu budú vytvorené (a budú realizovať opatrenia KIB).

Primárne opatrenia kybernetickej bezpečnosti chránia IS KURK, ktoré sú určené na prevádzkovanie univerzitných služieb. Z vyššie definovaných spôsobov realizácie cieľov (viď kapitola 3 Popis navrhovaného riešenia) je zrejmé, o aké komponenty zabezpečenia pôjde - firewally, multifaktorové overovanie, centrálny logovací nástroj, nástroj na sledovanie prevádzkových parametrov siete, nástroje na detekciu v sieti a na hranici siete, záložná kópia prevádzkových dát, kompletná dokumentácia podľa ZoKB vrátane BCM plánov, test zraniteľností interných aj externých adries ako aj nezávislý audit kybernetickej bezpečnosti.



Aplikačná architektúra riešenia

4.1 Biznis vrstva

Predmetom realizácie projektu bude zavedenie a IT podpora nasledovných business procesov:

- Riadenie prevádzky siete a informačného systému
- Zaznamenávanie, monitorovanie a riešenie incidentov kybernetickej bezpečnosti
- Zabezpečovanie kontinuity prevádzky

Okrem samotného zabezpečenia opatrení KIB v zmysle zákona o kybernetickej bezpečnosti a zákona o ISVS sa projekt bude dotýkať prakticky všetkých biznis procesov, ktoré sú vykonávané na KURK, a ktoré sú realizované prostredníctvom informačných systémov KURK za účelom poskytovania univerzitných služieb.

4.1.1 Prehľad koncových služieb – budúci stav:

Táto kapitola je irelevantná pre predmet projektu – implementácia bezpečnostných riešení. Nejde o agendový alebo iný informačný systém verejnej správy.

Projekt nerealizuje koncové služby pre zamestnancov a študentov. 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.

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 KURK 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 základnej služby. V aplikačnej vrstve je potrebné uvažovať o FrontEnd (verejných) častiach služby a Back-Office (neverejných častiach) služby.

Implementované komponenty budú v prípade KURK inštalované on-site, čiže dodávané služby nebudú dodávané ako služba od externého subjektu.

On-Site budú nasadené nasledovné opatrenia:

- Dokumentácia KB podľa vyhlášky a metodík
- NextGen Firewally v HA
- Analytické nástroje na sledovanie udalostí na perimetrovom firewalle
- Nástroje pre centrálnu správu logov a ich korelovanie
- Nástroj na kontrolu prevádzkových parametrov siete
- Backup konektor pre kritický systém eSPIS
- Systém na notifikáciu o existujúcich zraniteľnostiach
- Zariadenie na zabezpečenie zálohovania systémov
- Kryptografické nástroje na šifrovanie zálohovaných dát
- Plány kontinuity
- Interné a externé testy zraniteľností
- Nezávislý audit kybernetickej bezpečnosti

4.2.1 Rozsah informačných systémov – AS IS

V nasledujúcej tabuľke uvádzame ISVS, ktoré zabezpečujú prevádzku služieb KURK a budú 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_14310	akademický informačný systém AiS2		Prevádzkovaný a plánujem rozvíjať	Agendový	
isvs_14311	IS Abakus		Prevádzkovaný a plánujem rozvíjať	Agendový	
isvs_14312	IS Moodle - LMS		Prevádzkovaný a plánujem rozvíjať	Agendový	
isvs_14313	mediainfo		Prevádzkovaný a plánujem rozvíjať	Agendový	
isvs_14314	E-SPIS		Prevádzkovaný a plánujem rozvíjať	Agendový	
isvs_14315	CMS systém		Prevádzkovaný a plánujem rozvíjať	Prezentačný	

4.2.2 Rozsah informačných systémov – TO BE

Táto kapitola je irelevantná pre predmet projektu – implementácia bezpečnostných riešení. Nejde o agendový alebo iný informačný systém verejnej správy.

V rámci projektu vznikne jeden nový ISVS – Informačný systém kybernetickej bezpečnosti KURK, ktorý je spoločným označením pre všetky parciálne komponenty vytvorené v rámci tohto projektu. Nepôjde o IS v skutočnom slova zmysle – pôjde o súbor samostatných technologických opatrení, HW a SW, ktoré budú spoločne zabezpečovať požadovanú úroveň KIB KURK ako poskytovateľa univerzitných služieb.

4.2.3 Využívanie nadrezortných a spoločných ISVS – AS IS

Projekt resp. ním realizovaný ISVS 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 resp. ním realizovaný ISVS 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 resp. ním realizovaný ISVS nebude integrovaný na iné ISVS.

4.2.6 Aplikačné služby pre realizáciu koncových služieb – TO BE

Táto kapitola je irelevantná pre predmet projektu – implementácia bezpečnostných riešení. Nejde o agendový alebo iný informačný systém verejnej správy.

4.2.7 Aplikačné služby na integráciu – TO BE

Predmetom realizácie projekt resp. ním realizovaného ISVS nebudú žiadne služby určené na integráciu v rámci TO BE stavu.

4.2.8 Poskytovanie údajov z ISVS do IS CSRÚ – TO BE

Projekt resp. ním realizovaný ISVS nebude poskytovať údaje z ISVS do IS CSRÚ.

4.2.9 Konzumovanie údajov z IS CSRU – TO BE

Projekt resp. ním realizovaný ISVS nebude konzumovať údaje z IS CSRU.

4.3 Dátová vrstva

Z pohľadu dátového modelu nejde o typické biznis (agendové) dáta ale o dáta typu:

- Bezpečnostná dokumentácia a politiky, postupy, analýzy, reporty a pod. – ako výstupy aktivity projektu určené pre ďalšie riadenie rozvoja KIB,
- Bezpečnostné konfigurácie a bezpečnostné dáta (napr. logy) – pre fungovanie jednotlivých bezpečnostných komponentov.

Bezpečnostná dokumentácia a politiky, postupy, analýzy, reporty a pod. sú určené pre proces riadenia KIB. Bezpečnostné konfigurácie a bezpečnostné dáta slúžia pre správne fungovanie bezpečnostných modulov, t.j. jednotlivé komponenty tohto navrhovaného riešenia a zároveň reprezentujú vyhodnocovanie bezpečnostných udalostí a potenciálnych bezpečnostných incidentov.

4.3.1 Údaje v správe organizácie

Projekt resp. ním realizovaný ISVS nebude priamo zabezpečovať správu údajov KURK, bude spravovať iba údaje nevyhnutné na zabezpečenie KIB KURK (napríklad údaje logov zo SIEM, informácie o riešení incidentov KIB, zoznam oprávnení a pod.).

Z toho dôvodu neuvádzame namapovanú štruktúru údajov v správe KURK.

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 študenti resp. informácie o nich atď. Systém bude viesť evidenciu informačných aktív, analýza rizík, systémových logov a reporty KIB.

Takto uvedené skutočnosti teda môžeme - v snahe definovať objekty evidencie - prezentovať nasledovne:

ID OE	Objekt evidencie - názov	Objekt evidencie - popis	Referencovateľný identifikátor URI dátového prvku
1	Evidencia informačných aktív	Evidencia informačných aktív obsahuje informácie o všetkých informačných aktívach, ktoré sú potrebné pre chod univerzity. Pre jednotlivé aktíva sú určení vlastníci a administrátori.	
2	Analýza rizík	Analýza rizík obsahuje kompletnú analýzu rizík identifikovaných informačných aktív s prihliadnutím na triádu CIA.	
3	Systémové logy	Záznamy z dôležitých systémov univerzity, ktoré sú ukladané z dôvodu ich analýzy a korelácie.	
4	Reporty KIB	Objekt, ktorý za vybrané obdobie (deň, týždeň, mesiac) sumarizuje štatistické údaje relevantné z pohľadu kybernetickej bezpečnosti.	

4.3.3 Referenčné údaje

V rámci projektu ani ním realizovaného ISVS nebudú využívané referenčné údaje ani projekt resp. ním realizovaný ISVS nebude poskytovať referenčné údaje.

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

V rámci projektu ani ním realizovaného ISVS 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.

4.3.5 Otvorené údaje

V rámci projektu ani ním realizovaného ISVS nebudú vytvárané otvorené údaje.

4.3.6 Analytické údaje

V rámci projektu ani ním realizovaného ISVS nebudú vytvárané analytické údaje.

4.3.7 Moje údaje

V rámci projektu ani ním realizovaného ISVS 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

Predpokladané výkonnostné parametre a kapacitné požiadavky sú, tam kde je to relevantné, uvedené v popise aplikačnej architektúry jednotlivých aplikačných funkcií a aplikačných modulov.

Parameter	Jednotky	Predpokladaná hodnota	Poznámka
Počet interných používateľov	Počet	2 500	Jedná sa študentov denného, ako aj externého štúdia.
Počet súčasne pracujúcich interných používateľov v špičkovom zaťažení	Počet	500	Jedná sa o zamestnancov žiadateľa.
Počet externých používateľov (internet)	Počet	25 000	Jedná sa, ako o bývalých študentov a zamestnancov prevádzkovateľa IS, tak o laickú, ako aj verejnosť odbornú.
Počet externých používateľov používajúcich systém v špičkovom zaťažení	Počet	25 000	Maximálny počet používateľov interných a aj externých, ktorí sa môžu prihlásiť naraz, či už ako poskytovatelia (zamestnanci) alebo konzumenti (študenti).

4.4.3 Návrh riešenia technologickej architektúry

Predmetom plnenia bude:

1.Organizácia kybernetickej a informačnej bezpečnosti

- Vypracovanie bezpečnostnej politiky pre univerzitu ohľadom riadenia, kontroly a vyhodnocovania stavu kybernetickej bezpečnosti na univerzite.
- Vytvorenie, resp. aktualizácia kompletnej bezpečnostnej dokumentácie podľa požiadaviek ZoKB Prílohy č. 1 k vyhláške č. 362/2018 Z. z. Vypracovaná dokumentácia bude pokrývať všetky požadované oblasti požadovanej legislatívy. Pri vypracovávaní dokumentácie sa bude vychádzať z metodík vydaných MIRRI.

2.Riadenie rizík

- Kompletná identifikácia informačných aktív univerzity, vytvorenie katalógu aktív s určením vlastníkov a administrátorov jednotlivých aktív. Vypracovanie zoznamu hrozieb a ohodnotenie dopadov na aktíva z pohľadu triády CIA.
- Vypracovaný bude katalóg informačných aktív s určením vlastníkov a administrátorov jednotlivých aktív. Vypracovaný bude katalóg hrozieb a rizík a na základe týchto katalógov bude vypracovaná analýza rizík pre jednotlivé aktíva.
- Vypracovanie smernice pre riadenie rizík, podľa ktorej bude vykonávaná analýza rizík informačných systémov univerzity

3. Personálna bezpečnosť

- Vypracovanie postupov pri nástupe a odchode zamestnanca primárne z pohľadu prideľovania a odoberania prístupov do informačných systémov univerzity.
- Vypracovanie smernice pre koncových užívateľov a administrátorov, podľa ktorej sa bude riadiť bezpečnosť pri narábaní s pridelenými výpočtovými prostriedkami a pri prístupe do informačných systémov univerzity.

4. Riadenie prístupov

- Vypracovanie smernice pre riadenie prideľovania bezpečnostných rolí a úrovní prístupov pre interných a externých zamestnancov z dôvodu umožnenia prístupu k informačným systémom univerzity

5. Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami

- Určenie a revízia dodávateľských zmlúv s tretími stranami, ktoré majú vplyv na poskytovanie kritických systémov organizácie. Návrh zmien v zmluvách týkajúcich sa oblasti kybernetickej bezpečnosti.
- Vypracovanie návrhu dodatku k zmluve s treťou stranou, ktorý bude pokrývať požiadavky ZoKB, ktoré sa týkajú dodávateľských vzťahov.

6. Bezpečnosť pri prevádzke informačných systémov a sietí

- Analýza a návrh pravidiel a politík pre koncové stanice v závislosti od ich použitia. Činnosť pozostáva z identifikácie use cases a návrhu na optimálne zabezpečenie identifikovaných kategórií pracovných staníc (učebne – študentské, prezentačné PC, zamestnanci pedagogickí, administratívni).
- Vypracovanie smernice pre administrátorov, podľa ktorej sa budú riadiť pri správe interných systémov univerzity. Vypracovanie postupov pre aplikovanie zmien v informačných systémoch univerzity a smerníc pre zaznamenávanie prevádzkových a bezpečnostných nastavení systémov.
- Obstaranie služieb pre potreby správy prevádzkovej zálohy, kópie archivačnej zálohy a kópie inštalačných médií. Implementácia archivačného konektora pre existujúce systémy ISVS eSPIS

7. Hodnotenie zraniteľností a bezpečnostné aktualizácie

- Vypracovanie interného riadiaceho dokumentu upravujúceho proces riadenia implementácie bezpečnostných aktualizácií a záplat.

8. Ochrana proti škodlivému kódu

- Vypracovanie smernice ohľadom implementácie a správy systémov, ktoré majú za úlohu chrániť organizáciu pred škodlivým kódom.
- Vypracovanie interného riadiaceho dokumentu pre administrátorov ohľadom ochrany koncových bodov pred škodlivým kódom

9. Sieťová a komunikačná bezpečnosť

- Implementácia a konfigurácia perimetrového firewallu za účelom zabezpečenia bezpečného oddelenia internej siete a internetu. Úlohou tohto firewallu bude aj riešiť bezpečný prestup medzi segmentami siete a taktiež bude zabezpečovať bezpečný vzdialený prístup do siete na základe VPN spojení s overovaním pomocou dvojfaktorovej autentizácie
- Vypracovanie interného riadiaceho dokumentu upravujúceho pravidlá sieťovej a komunikačnej bezpečnosti
- Implementácia dohľadového nástroja, ktorý sleduje a identifikuje sieťové spojenia na hranici s vonkajšou sieťou, vytvára prehľady o prenesených dátach, o podozrivých prístupoch na škodlivé stránky a je schopný vytvárať automatizované reporty z pohľadu dodržiavania bezpečnostných smerníc.
- Implementácia sond detekcie a prevencie prieniku, najmä na serveroch podporujúcich základné služby informačných technológií verejnej správy.

10. Zaznamenávanie udalostí a monitorovanie

- Zaobstaranie, implementácia a konfigurácia centrálneho logovacieho systému, ktorý bude bezpečným spôsobom zbierať, vyhodnocovať, vizualizovať a ukladať systémové logy zo všetkých dôležitých systémov univerzity
- Vypracovanie dokumentácie spôsobu monitorovania a fungovania centrálneho log manažment systému a centrálneho nástroja na bezpečnostné monitorovanie a zadefinovanie spôsobu evidencie prevádzkových záznamov, ich vyhodnocovania, spôsobu hlásenia podozrivej aktivity, zodpovednej osoby a ďalších povinností
- Implementácia a konfigurácia monitorovacieho nástroja, ktorý bude monitorovať prevádzkové parametre prevádzkovaných systémov a ktorý bude alertovať v prípade, že dôjde k odchýlke týchto parametrov od bežnej prevádzky.
- Tento cieľ bude naplnený implementáciou pohľadového systému pre sledovanie prevádzkových parametrov všetkých systémov podieľajúcich sa na prevádzke alebo podpore poskytovaných služieb: sieťových zariadení, serverov, aplikácií a ďalších IT prostriedkov. Robustná open-source platforma určená na monitorovanie sietí, serverov a aplikácií. Jeho hlavnou úlohou je poskytovať komplexný prehľad o výkone a dostupnosti vašej IT infraštruktúry v reálnom čase, čo umožňuje efektívne predchádzať problémom skôr, než negatívne ovplyvnia chod IKT. Systém musí podporovať široké spektrum metód na zber dát vrátane agentov, SNMP, IPMI, JMX, trapy a log súbory, čo zaručí flexibilitu a kompatibilitu s rôznymi zariadeniami a aplikáciami. V prípade potreby musí byť možné využiť proxy, ktorý zníži záťaž na hlavný server a umožní efektívne monitorovanie geograficky vzdialených lokalít.
- Kľúčové požadované vlastnosti:
    - konfigurovateľné upozornenia a notifikácie, ktoré môžu byť zasielané prostredníctvom emailov, SMS, skriptov alebo webhookov,
    - vizualizácia dát pomocou grafov, máp, prehľadov a dashboardov,
    - šifrovaná komunikácia medzi serverom, agentmi a užívateľom, čo zaručuje ochranu citlivých informácií,
    - podpora autentifikácie a rôznych úrovní prístupových práv zabezpečí, že prístup k monitorovacím dátam budú len oprávnené osoby.

11. Fyzická bezpečnosť a bezpečnosť prostredia

- Obstaranie a implementácia dátového úložiska pre potreby zálohy prevádzkových dát a archivačnej kópie pomocou obstarania záložných kapacít pre ukladanie prevádzkových dát, umiestnené v zabezpečenom priestore bezpečne vzdialenom zálohovanému zabezpečenému priestoru.
- Tento bod bude splnený dodávkou HW zariadení na rozšírenie aktuálne prevádzkovaného diskového poľa NetApp. Potrebným navýšením diskových kapacít pre ukladanie zálohy prevádzkových dát a pomocou existujúceho softvéru na zálohovanie.
- - Dodávka hardvéru na rozšírenie aktuálneho diskového poľa.
- - Realizácia inštalačných a konfiguračných služieb, ktoré zabezpečia možnosť ukladania zálohy prevádzkových dát, vrátane testovacej obnovy dát

12. Riešenie kybernetických bezpečnostných incidentov

- Vypracovanie štandardov a postupov riešenia kybernetických bezpečnostných incidentov, vrátane definovania zodpovedností zamestnancov a ďalších povinností, vypracovanie plánov a spôsobov riešenia kybernetických bezpečnostných incidentov

13. Kryptografické opatrenia

- Vypracovanie smernice pre kryptografické opatrenia, ktorá bude definovať používanie a uchovávanie informácií týkajúcich sa použitých prístupových hesiel a kľúčov, bezpečnostných certifikátov a ostatných bezpečnostných prvkov

14. Kontinuita prevádzky

- Vypracovanie stratégie a krízových plánov prevádzky na základe analýzy vplyvov kybernetického bezpečnostného incidentu na základnú službu. Vypracovanie dekompozície dôležitých služieb a vypracovanie BIA pre tieto služby, resp. systémy
- Vypracovanie plánov kontinuity prevádzky pre dva kritické systémy univerzity a ich prvotné otestovanie v reálnom prostredí organizácie a zapracovanie nedostatkov z výsledkov testovania.
- Vykonanie testovania navrhnutých plánov kontinuity a zapracovanie nedostatkov z výsledkov testovania

15. Audit a kontrolné činnosti

- Vypracovanie smernice pre posudzovanie bezpečnosti informačných systémov verejnej správy a ich vyhodnocovania.
- obstaranie prvého alebo opakovaného auditu kybernetickej bezpečnosti v súlade so zákonom o KB;

4.4.4 Využívanie služieb z katalógu služieb vládneho cloudu

Projekt ani ním realizovaný ISVS nebude využívať služby vládneho cloudu.

4.5 Bezpečnostná architektúra

V súčasnosti - ako vyplýva z projektového zámeru - nie sú opatrenia KIB KURK - 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

KURK 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 zvyšku 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 Dodávateľ 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.) takejto 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 ITVS.

7. Prevádzka a údržba

7.1 Prevádzkové požiadavky

Aktivita podpora Governance v oblasti KIB si nevyžaduje žiadnu budúcu prevádzku, nakoľko ide len o analytické a konzultačné práce, ktorých výstupy budú použité pre proces riadenia KIB (Governance). Výstupy Governance aktivít samozrejme tiež budú musieť byť udržiavané a rozvíjané, to by však malo byť realizované pomocou interných zamestnancov bez priameho vplyvu na rozpočet.

Prevádzka a údržba výstupov projektu sú spracované v projektovom zámere a časti 4. Architektúra riešenia projektu.

Prevádzka a údržba výstupov projektu nie sú predmetom ŽoNFP.

7.1.1 Úrovne podpory používateľov

Táto kapitola je irelevantná pre predmet projektu – implementácia bezpečnostných riešení. Nejde o agendový alebo iný informačný systém verejnej správy.

7.1.2 Riešenie incidentov – SLA parametre

Označenie naliehavosti incidentu:

Označenie naliehavosti incidentu	Závažnosť incidentu	Popis naliehavosti incidentu
A	Kritická	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.
B	Vysoká	Chyby a nedostatky, ktoré zapríčinia čiastočné zlyhanie systému a neumožňuje používať časť systému.
C	Stredná	Chyby a nedostatky, ktoré spôsobia čiastočné obmedzenia používania systému.
D	Nízka	Kozmetické a drobné chyby.

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
	Nízka - D	3	4	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	

7.2 Požadovaná dostupnosť IS:

Popis	Parameter	Poznámka
Prevádzkové hodiny	12 hodín	od 6:00 hod. - do 18:00 hod. počas pracovných dní
Servisné okno	10 hodín	od 19:00 hod. - do 5:00 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	98,5%	98,5% z 24/7/365 t.j. max ročný výpadok je 66 hod. Maximálny mesačný výpadok je 5,5 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.

8. Požiadavky na personál

Pre účely realizácie projektu sa zostavuje Riadiaci výbor (RV), v minimálne nasledovnom zložení:

- Predseda RV PaedDr. Ján Kamoďa, PhD.
- Vlastník procesov Ing. Vendelín Ružička
- Zástupca kľúčových používateľov Ing. Rudolf Kollár
- Projektový manažér Ing. František Horvát, PhD.

- Tajomník RV Ing. Jana Kollárová

Projektový tím objednávateľa:

- Manažér kybernetickej bezpečnosti Ing. Rudolf Kollár
- IT analytik Ing. Jana Kollárová
- IT architekt Ing. Vendelín Ružička
- Projektový manažér objednávateľa (PM) Ing. František Horvát, PhD.

Stručne zodpovednosti jednotlivých rolí:

Projektová rola: Biznis vlastník

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 401/2023 Z.z., Prílohou č.1 plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

Projektová rola: Projektový manažér objednávateľa (PM)

Zodpovedný za:

- Riadenie projektu podľa pravidiel stanovených vo Vyhláške 401/2023 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 401/2023 Z. 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 401/2023 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 401/2023 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

Projektová rola: KĽUČOVÝ POUŽIVATEĽ (end user)

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 401/2023 Z.z., Prílohou č.1
- Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu
- Realizáciu kvalitatívneho používateľského výskumu (nastavenie požiadaviek na regrutáciu, návrh scenára, vedenie rozhovoru a vyhodnotenie výskumu).
- Realizáciu kvantitatívneho používateľského výskumu (nastavenie požiadaviek na regrutáciu, návrh scenára, vedenie dotazníku a vyhodnotenie výskumu).
- Syntetizáciu biznis, technických a používateľských požiadaviek.
- Realizáciu formatívnych a sumatívnych testovaní použiteľnosti (nastavenie požiadaviek na regrutáciu, návrh scenára, vedenie rozhovoru a vyhodnotenie výskumu).
- Návrh informačnej architektúry a to najmä metódami triedenia kariet (card sorting), návrhom mapy stránky a screen flow.
- Tvorbu, testovanie a iteráciu prototypov – napr. pomocou Axure, Sketch, Figma alebo Adobe XD
- Mapovanie zákazníckych ciest
- Analýzu a návrh riešenia problematiky prístupnosti webových sídiel,
- Podporu a spoluprácu pri tvorbe Stratégie riadenia kvality (princípy, kritériá kvality),
- Spoluprácu pri vytváraní funkčných požiadaviek na výstupy z pohľadu dohľadu a UX,
- Vedenie a aktualizáciu príslušných projektových výstupov a registrov,
- Hodnotenie jednotlivých verzií výstupov projektu z pohľadu dohľadu, kontroly a UX v jednotlivých etapách,
- Vytváranie hodnotiacich kritérií na dohľad výstupov a príslušných záznamov, o ktorých reportuje projektovému manažérovi objednávateľa,
- Nastavenie a dohľad nad procesom testovania a pripomienkovanie stratégie testovania, plánov a testovacích scenárov,
- Účasť na kontrolných aktivitách počas implementácie výstupov
- Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 401/2023 Z.z., Prílohou č.1
- Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 401/2023 Z.z., Prílohou č.1
- Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

Projektová rola: IT analytik

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 401/2023 Z.z., Prílohou č.1
- Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

Projektová rola: IT architekt

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 401/2023 Z.z., Prílohou č.1
- Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

Projektová rola: manažér kybernetickej a informačnej bezpečnosti

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 401/2023 Z.z., Prílohou č.1 plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

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.

10. Prílohy

Bez príloh.