projekt_2660_Pristup_k_projektu_ramcovy

PRÍSTUP K PROJEKTU

Manažérsky výstup I-03

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

Povinná osoba	Univerzita Komenského v Bratislave
Názov projektu	Podpora v oblasti kybernetickej a informačnej bezpečnosti na regionálnej úrovni – Univerzita Komenského v Bratislave
Zodpovedná osoba za projekt	Ing. Rastislav Kulhánek, PhD.
Realizátor projektu	Univerzita Komenského v Bratislave
Vlastník projektu	Univerzita Komenského v Bratislave

Schvaľovanie dokumentu

Položka	Meno a priezvisko	Organizácia	Pracovná pozícia	Dátum	Podpis (alebo elektronický súhlas)
Vypracoval	Ing. Rastislav Kulhánek, PhD.	Univerzita Komenského v Bratislave	Manažér informačnej bezpečnosti	08.07.2024	

1. História dokumentu

Verzia	Dátum	Zmeny	Meno
0.1	*20.05.2024*	*Pracovný návrh*	Ing. Rastislav Kulhánek, PhD
1.0	*08..07.2024*	*Zapracovanie súladu s vyhláškou č. 401/2023 Z. z., finálna verzia v súlade so ŽoNFP*	Ing. Rastislav Kulhánek, 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 „Podpora v oblasti kybernetickej a informačnej bezpečnosti na regionálnej úrovni – verejná správa“ (ďalej len výzva) bude obsahovať opis navrhovaného riešenia, architektúru riešenia projektu na úrovniach biznis vrstvy, dátovej vrstvy, technologickej vrstvy, infraštruktúry navrhovaného riešenia a bezpečnostnej architektúry. Dokument tiež popisuje 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 nasledujúce základné typy požiadaviek:

Funkcionálne (používateľské) požiadavky majú nasledovnú konvenciu:

FRxx

- F funkčná užívateľská požiadavka
- xx číslo požiadavky

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

NRxx

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

Technické požiadavky majú nasledovnú konvenciu:

Txx

- T technická požiadavka
- xx číslo požiadavky

3. Popis navrhovaného riešenia

Navrhované riešenie vychádza z aktuálnych zistení posledného auditu kybernetickej bezpečnosti.
Závery auditu kybernetickej bezpečnosti definujú aktuálny stav a potreby, ktoré je nevyhnuté riešiť pre dosiahnutie súladu úrovne kybernetickej a informačnej bezpečnosti (ďalej len KIB) so zákonom č. 69/2018 Z. z. O kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len “zákon o kybernetickej bezpečnosti), Zákonom č. 95/2019 Z. z. O informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len “zákon o ISVS”), vyhláškou 362/2018 Z.z. o obsahu bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len vyhláška č. 362 /2018 Z. z.) a ďalšími súvisiacimi predpismi.
Navrhované riešenie tiež zohľadňuje požiadavky definované v smernici európskej únie NIS2.

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

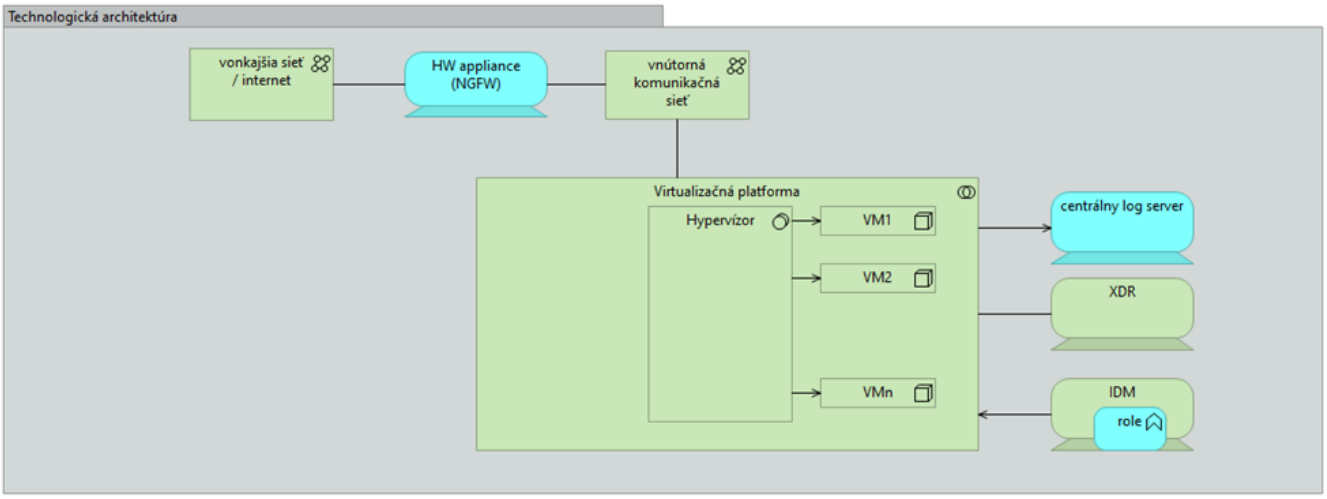
ID	Názov cieľa	Názov strategického cieľa*	Spôsob realizácie strategického cieľa

1	Zabezpečenie organizácie kybernetickej a informačnej bezpečnosti Vytvorenie, resp. aktualizácia kompletnej bezpečnostnej dokumentácie podľa požiadaviek ZoKB Prílohy č. 1 k vyhláške č. 362/2018 Z. z. Cieľ realizovaný v zmysle oprávnených podaktivít: • organizácia kybernetickej a informačnej bezpečnosti • riadenie rizík • personálna bezpečnosť • riadenie prístupov • riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami • bezpečnosť pri prevádzke informačných systémov a sietí • ochrana proti škodlivému kódu • fyzická bezpečnosť a bezpečnosť prostredia • riešenie kybernetických bezpečnostných incidentov • kryptografické opatrenia • kontinuita prevádzky	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. Bližšie popísané pri Predmet plnenia – 1.Vytvorenie, resp. aktualizácia kompletnej bezpečnostnej dokumentácie podľa požiadaviek ZoKB Prílohy č. 1 k vyhláške č. 362/2018 Z. z.
2	Zabezpečenie organizácie kybernetickej a informačnej bezpečnosti Zvyšovanie bezpečnosti zamestnancov pomocou nasadenia manažmentu rolí v centrálnom IDM riešení Cieľ realizovaný v zmysle oprávnených podaktivít: riadenie prístupov	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Aktualizácia centrálneho nástroja na správu a overovanie identity, nástroja na riadenie prístupových oprávnení vrátane privilegovaných prístupových práv a kontroly prístupových účtov a prístupových oprávnení. Bližšie popísané pri Predmet plnenia – 2. Zvyšovanie bezpečnosti zamestnancov pomocou nasadenia manažmentu rolí v centrálnom IDM riešení (midpoint role based identity mangement)
3	Zabezpečenie organizácie kybernetickej a informačnej bezpečnosti Zvýšenie sieťovej a komunikačnej bezpečnosti nasadením a implementáciou perimetrového firewallu Cieľ realizovaný v zmysle oprávnených podaktivít: • Sieťová a komunikačná bezpečnosť • Zaznamenávanie udalostí a monitorovanie	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Implementácia nástrojov na ochranu integrity sietí, ktoré zabezpečujú riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami, implementácia segmentácie sietí, implementácia alebo obnova firewall-u, revízia firewall pravidiel. Bližšie popísané pri Predmet plnenia – 3. implementácia firewall-u Implementácia centrálneho Log manažment systému pre zber a ukladanie logov z jednotlivých informačných systémov. Bližšie popísané pri Predmet plnenia – 4.Implementácia log manažmentu
4	Zabezpečenie organizácie kybernetickej a informačnej bezpečnosti 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)	Obstaranie prvého alebo opakovaného auditu kybernetickej bezpečnosti v súlade so zákonom o KB. Bližšie popísané pri Predmet plnenia – 5. Nezávislý audit kybernetickej bezpečnosti

4. Architektúra riešenia projektu

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

Obrázok1:

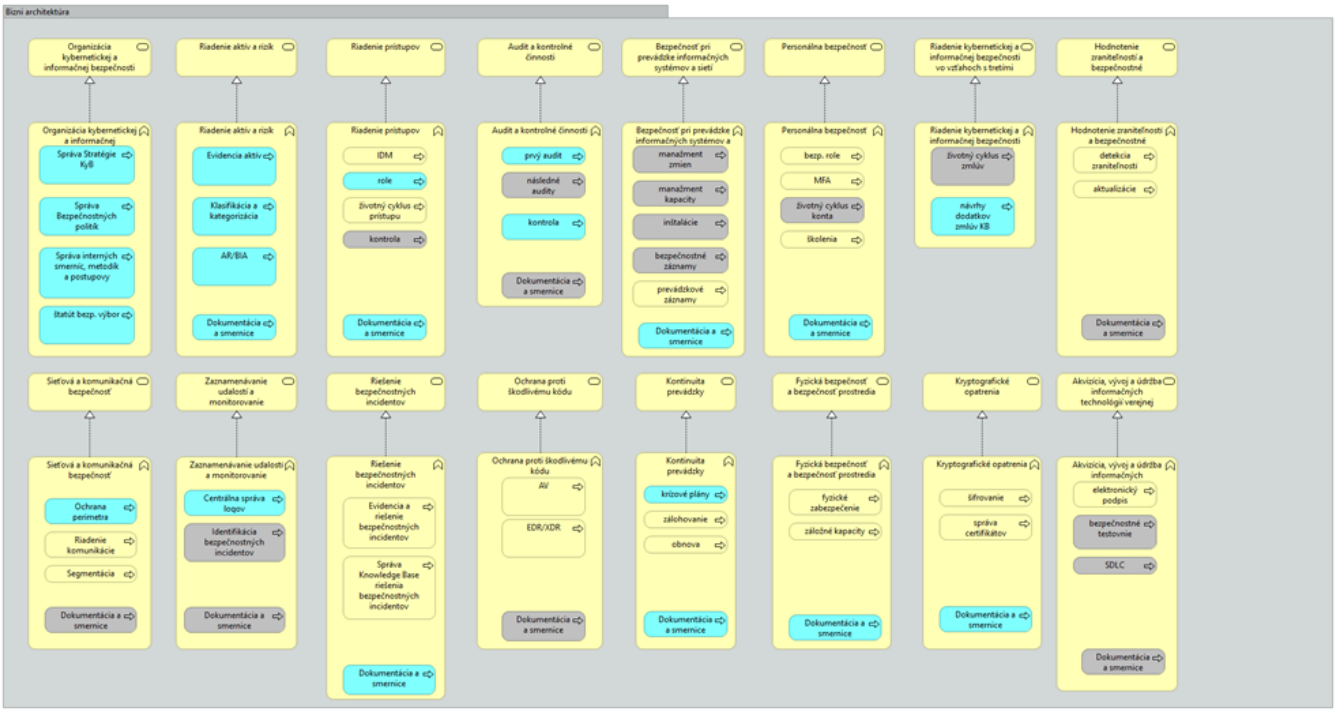


4.1 Biznis vrstva

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

- Organizácia kybernetickej a informačnej bezpečnosti
- Riadenie rizík
- Personálna bezpečnosť
- Riadenie prístupov
- Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami
- Bezpečnosť pri prevádzke informačných systémov a sietí
- Ochrana proti škodlivému kódu
- Sieťová a komunikačná bezpečnosť
- Zaznamenávanie udalostí a monitorovanie
- Fyzická bezpečnosť a bezpečnosť prostredia
- Riešenie kybernetických bezpečnostných incidentov
- Kryptografické opatrenia
- Kontinuita prevádzky

Audit a kontrolné činnostiOkrem 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 UK v Bratislave, a ktoré sú realizované prostredníctvom informačných systémov UK za účelom poskytovania univerzitných služieb.



4.1.1 Prehľad koncových služieb – budúci stav:

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

Z toho vyplýva, že „koncovou službou“ projektu bude samotná služba kybernetickej a informačnej bezpečnosti, poskytovaná organizácii. Služba je poskytovaná automatizovane IT technológiami KIB.

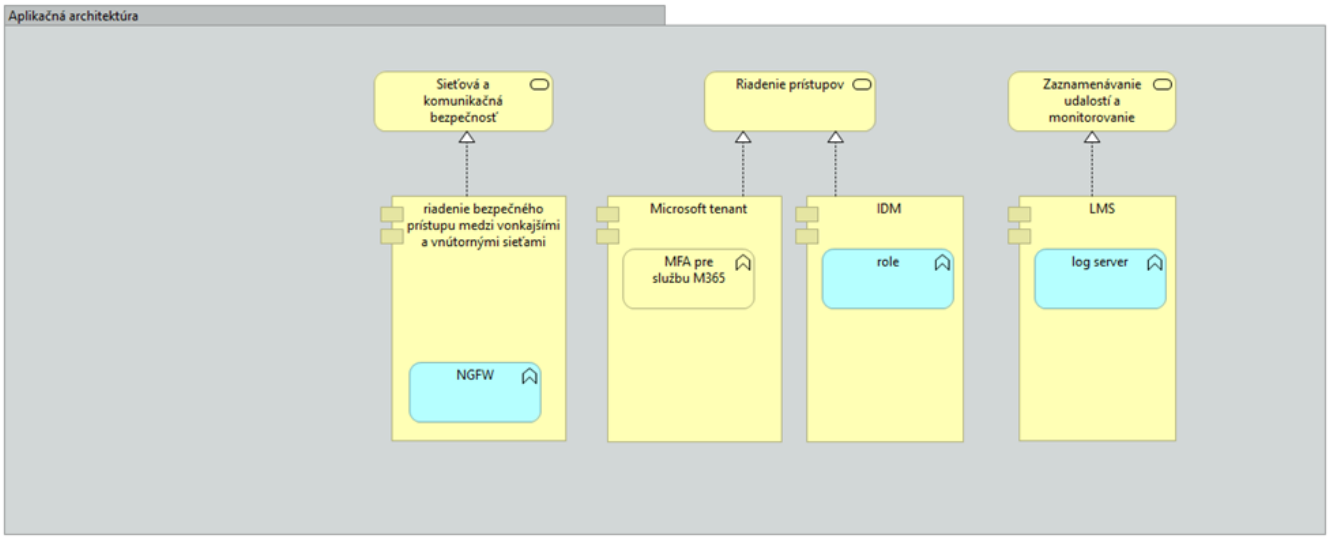
4.1.2 Jazyková podpora a lokalizácia

Projekt bude realizovaný v podobe dokumentov (politiky, plány, stratégie, analýza atď.), ktoré budú akceptované v slovenskom jazyku prípadne na základe dohody v anglickom jazyku. Implementované softvérové riešenia budú akceptované v slovenskej, českej alebo v anglickej mutácií. Dodané softvérové riešenia, alebo hardvérové komponenty musia mať návod v slovenskom, alebo anglickom jazyku. Projektová dokumentácia bude vyhotovovaná v slovenskom jazyku.

Výstupy z prevádzky systémov budú akceptované v slovenskom a anglickom jazyku, niektoré čiastkové výstupy (napr. Logy incidentov) 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.



4.2.1 Rozsah informačných systémov – AS IS TA SR

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_14301	Kamerový systém		Prevádzkovaný a plánujem rozvíjať	Agendový	
isvs_10452	Webový portál Univerzity Komenského		Prevádzkovaný a plánujem rozvíjať	Prezentačný	
isvs_14300	Systém pre správu identít		Prevádzkovaný a plánujem rozvíjať	Integračný	
isvs_14298	e-learning		Prevádzkovaný a plánujem rozvíjať	Agendový	
isvs_14297	Akademický informačný systém		Prevádzkovaný a plánujem rozvíjať	Agendový	

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.

4.2.3 Využívanie nadrezortných a spoločných ISVS – AS IS

V rámci projektu a realizovaného ISVS sa nebudú využívať nadrezortné a spoločné ISVS.

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

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

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

Jedinou aplikačnou službou nového ISVS bude Aplikačná služba kybernetickej a informačnej bezpečnosti UK, ktorá je spoločným pomenovaním všetkých implementovaných opatrení v rámci realizácie projektu.

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

4.3.1 Údaje v správe organizácie

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

Z toho dôvodu neuvádzame namapovanú štruktúru údajov v správe UK.

4.3.2 Dátový rozsah projektu - Prehľad objektov evidencie - TO BE

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

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
OE_01	Prístupové oprávnenia	Evidencia prístupových práv zamestnancov a spolupracovníkov UK k jednotlivým IS UK, evidencia práv prístupov k webovým aplikáciám, evidencia všetkých informácií, ktoré sú potrebné pre riadenie prístupov v rámci IS UK	Nemá
OE_02	Záznam kybernetického incidentu	Záznamy (logy) log server, ktoré budú zaznamenávané zo všetkých sieťových zariadení slúžia na dohľadanie udalostí pri kybernetickom incidente	Nemá

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 sa bude narábať s údajmi zamestnancov UK a externých spolupracovníkov UK pri aktualizácii Identity Management. Rozsah spracovania týchto údajov nebude nad rámec súčasného rozsahu.

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, ako aj ďalších zákonov a vyhlášok súvisiacich s KIB organizácii verejnej správy. Tiež je potrebné zohľadniť požiadavky prezentované smernicou európskej únie NIS2.

4.4.2 Požiadavky na výkonnostné parametre, kapacitné požiadavky – TO BE

Parameter	Jednotky	Predpokladaná hodnota	Poznámka
Počet interných používateľov	Počet	4878	
Počet súčasne pracujúcich interných používateľov v špičkovom zaťažení	Počet	4878	
Počet externých používateľov (internet)	Počet	84455	
Počet externých používateľov používajúcich systém v špičkovom zaťažení	Počet	35000	

4.4.3 Návrh riešenia technologickej architektúry pre UK

Z technologického hľadiska pôjde o nasledovné realizácie:

1.Vytvorenie, resp. aktualizácia kompletnej bezpečnostnej dokumentácie podľa požiadaviek ZoKB Prílohy č. 1 k vyhláške č. 362/2018 Z. z.

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. Pri vypracovávaní dokumentácie sa bude vychádzať z metodík vydaných MIRRI.

- vypracovanie alebo aktualizácia bezpečnostnej dokumentácie vrátane rozsahu a spôsobu plnenia všeobecných bezpečnostných opatrení,
- vypracovanie špecifických interných riadiacich aktov pre vybrané oblasti kybernetickej a informačnej bezpečnosti,
- vypracovanie štatútu bezpečnostného výboru,
- identifikácia aktív súvisiacich so zariadeniami na spracovanie informácií a centrálne zaznamenávanie inventáru týchto aktív podľa ich hodnoty vrátane určenia ich vlastníka, ktorý definuje požiadavky na ich dôvernosť, dostupnosť a integritu,
- riadenie rizík pozostávajúce z identifikácie zraniteľností, identifikácie hrozieb, identifikácie a analýzy rizík s ohľadom na aktívum, určenie vlastníka rizika, implementácie organizačných a technických bezpečnostných opatrení, analýzy funkčného dopadu a pravidelného preskúmavania identifikovaných rizík v závislosti od aktualizácie prijatých bezpečnostných opatrení,
- vypracovanie interného riadiaceho aktu riadenia rizík kybernetickej a informačnej bezpečnosti,
- vypracovanie postupov pri zaradení osoby do niektorých z bezpečnostných rolí, zavedenie plánu rozvoja bezpečnostného povedomia a vzdelávania, vypracovanie spôsobov hodnotenia účinnosti plánu rozvoja bezpečnostného povedomia, určenie pravidiel a postupov na riešenie prípadov porušenia bezpečnostnej politiky, zavedenie postupov pri skončení pracovnoprávneho vzťahu alebo iného obdobného vzťahu, zavedenie postupov pri porušení bezpečnostných politík,
- vypracovanie alebo aktualizácia interného riadiaceho aktu s bezpečnostnými zásadami pre koncových používateľov,
- vypracovanie postupov a procesov upravujúcich personálnu bezpečnosť organizácie prostredníctvom interného riadiaceho aktu,
- vypracovanie zásad riadenia prístupov osôb k sieti a informačnému systému;
- vypracovanie postupov a procesov upravujúcich riadenie prístupov organizácie.
- vypracovanie návrhov dodatkov zmlúv s treťou stranou spolu s návrhom potrebných úprav na zabezpečenie súladu so zákonom KB,
- vypracovanie interného riadiaceho aktu upravujúceho zásady kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami,
- zavedenie opatrení a interného riadiaceho aktu v oblasti riadenia zmien, riadenia kapacít, inštalácie softvéru v sieťach a informačných systémoch, inštalácia zariadení v sieťach a informačných systémoch, zaznamenávanie bezpečnostných záznamov a zaznamenávanie a vyhodnocovanie prevádzkových záznamov,
- vypracovanie a implementácia pravidiel súvisiace s ochranou proti škodlivému kódu;
- vypracovanie interného riadiaceho aktu upravujúceho fyzickú bezpečnosť a bezpečnosť prostredia,
- vypracovanie štandardov a postupov riešenia kybernetických bezpečnostných incidentov, vrátane definovania zodpovedností zamestnancov a ďalších povinností,
- vypracovanie interného riadiaceho aktu obsahujúceho a upravujúceho povinnosti týkajúce sa riešenia kybernetických bezpečnostných incidentov,
- vypracovanie plánov a spôsobov riešenia kybernetických bezpečnostných incidentov.
- vypracovanie a implementácia interného riadiaceho aktu upravujúceho používanie kryptografických prostriedkov a šifrovania,
- definovanie pravidiel využitia kryptografických prostriedkov používajúcich dostatočne odolné kryptografické mechanizmy na ochranu údajov pri ich prenose alebo uložení v rámci sietí a informačných systémov,
- vypracovanie stratégie a krízových plánov prevádzky na základe analýzy vplyvov kybernetického bezpečnostného incidentu na základnú službu,
- vypracovanie plánov kontinuity prevádzky a ich prvotné otestovanie v reálnom prostredí organizácie a zapracovanie nedostatkov z výsledkov testovania,
- vypracovanie interného riadiaceho aktu obsahujúceho a upravujúceho kontinuitu prevádzky následkom kybernetického bezpečnostného incidentu alebo inej krízovej situácie,
- vypracovanie postupov zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu alebo inej krízovej situácie.

2. Zvyšovanie bezpečnosti zamestnancov pomocou nasadenia manažmentu rolí v centrálnom IDM riešení

Aktualizácia centrálneho nástroja na správu a overovanie identity, nástroja na riadenie prístupových oprávnení vrátane privilegovaných prístupových práv a kontroly prístupových účtov a prístupových oprávnení - midpoint role based identity mangement

UK rozšíri existujúce IDM riešenie na správu identít používateľov a nastaví zvýšenie bezpečnosti a prehľadnosti identít pri využití manažmentu rolí. UK sa v minulosti rozhodola použiť open source provisioning systém midPoint, ktorý je vyvíjaný na Slovensku a je mu poskytovaná podpora výrobcom. V rámci univerzitných interných kapacít bol spustený pilotný projekt proof of concept (PoC) na overenie vhodnosti tohto nástroja už v roku 2022 a následne v rámci VO vysúťažený presun niekoľkých systémov do tohto prostredia v roku 2024. Výsledkom projektu je úspešná implementácia procesov. Teraz je nevyhnutné, aby systém podporoval manažment samotných rolí v jednotlivých systémoch, ktoré univerzita nie je schopná realizovať svojpomocne.

Tento projekt sa dotýka a umožní prácu:

- počet aktívnych študentov: 23 400
- počet aktívnych zamestnaneckých pomerov: 5 700
- počet aktívnych externistov: 620
- počet alumných študentov a zamestnancov evidovaných od roku 2006: 244 000
- počet ubytovaných študentov: cca 10000

Očakávaný stav

- Revízia a úprava aktuálnej konfigurácie

- Implementácia, testovanie a nasadenie nových funkcionalít,
- Funkcionality a práce budú rozdelené do fáz, najmä pre lepšiu kontrolu vykonávania a plnenia tejto zákazky.

- 8x5 podpora existujúceho riešenia vrátane jeho rozšírení popísané nižšie predplatený na jeden kalendárny rok od uvedenia danej fázy systému do ostrej prevádzky.
- Zaškolenie IDM administrátora na bežné prevádzkové úlohy.
- Dodávka konfigurácie systému vrátane midscribe dokumentácie.
- Možnosť ďalšieho rozšírenia podľa potreby cez zmenové požiadavky za dohodnutý MD rate, ktorý bude hradiť univerzita zo svojho rozpočtu.

Fáza 1

- Návrh a implementácia integrácie systému midPoint s aplikáciou VoIP telefonia (Obelix)
- Návrh a implementácia rozšírenia existujúcej integrácie medzi systémom midPoint a aplikáciou ALVAO Service Desk (SD)
- Návrh a implementácia rozšírenia existujúcej integrácie systému midPoint s aplikáciou Microsoft Endpoint Manager (MSEM),

Fáza 2

- Návrh a implementácia rozšírenia rozšírenia existujúcej integrácie systému midPoint s aplikáciou Marquet DNS pre IKT (DNS)
- Vytvorenie aplikačných rolí pre Univerzitný WEB v systéme midPoint a konfiguráciu procesov, ktorá v systéme midPoint umožní pridelenie resp. odoberanie týchto rolí.
- Návrh a konfigurácia funkcionality žiadostí o role a nákupného košíku
- Návrh a konfigurácia rozšírenia pre schvaľovacie procesy

Fáza 3

- Návrh a implementácia rozšírenia existujúcej integrácie systému midPoint s aplikáciou Turnikety - prístupový systém COMINFO (PS)
- Vytvorenie aplikačných rolí pre ESET Antivírus v systéme midPoint a konfiguráciu procesov, ktoré v systéme midPoint umožní pridelenie resp. odoberanie týchto rolí.
- Vytvorenie aplikačných rolí pre Kamerový systém v systéme midPoint a konfiguráciu procesov, ktoré v systéme midPoint umožní pridelenie resp. odoberanie týchto rolí.
- Vytvorenie aplikačných rolí pre systém OverSi v systéme midPoint a konfiguráciu procesov, ktoré v systéme midPoint umožní pridelenie resp. odoberanie týchto rolí.
- Vytvorenie aplikačných rolí pre systém Absolventi UK v systéme midPoint a konfiguráciu procesov, ktoré v systéme midPoint umožní pridelenie resp. odoberanie týchto rolí.
- Vytvorenie aplikačných rolí pre systém Evidencia zmlúv v systéme midPoint a konfiguráciu procesov, ktoré v systéme midPoint umožní pridelenie resp. odoberanie týchto rolí.
- Vytvorenie aplikačných rolí pre systém E-ubytovanie v systéme midPoint a konfiguráciu procesov, ktoré v systéme midPoint umožní pridelenie resp. odoberanie týchto rolí.
- Vytvorenie aplikačných pre systém Kontakty v systéme midPoint a konfiguráciu procesov, ktoré v systéme midPoint umožní pridelenie resp. odoberanie týchto rolí.

Fáza 4

- Rozšírenie existujúcej integrácie systému midPoint s akademickým informačným systémom AIS2
- Návrh a konfigurácia funkcionality certifikácií a re-certifikácií pre opätovné schválenie existujúcich prístupov.
- Návrh a konfigurácia funkcionality, ktorá zabezpečí automatickú deaktivácia prístupov keď osobe skončí súvisiaci zamestnanecký pomer.

3. Implementácia firewall-u

Implementácia nástrojov na ochranu integrity sietí, ktoré zabezpečujú riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami, implementácia segmentácie sietí, implementácia alebo obnova firewall-u, revízia firewall pravidiel - Obstaranie HW, SW, služby, zaškolenia.

Na univerzite nie je v súčasnosti využívaný perimetrový firewall s pokročilými bezpečnostnými funkcionalitami. Toto predstavuje značné riziko v kybernetickej bezpečnosti, nakoľko nie je možné odhaľovať a zamedzovať kybernetickým hrozbám na rozhraní internej siete univerzity a internetu. Za účelom zvýšenia bezpečnosti budú zakúpené a implementované sieťové zariadenia zabezpečujúce oddelenie internej siete od internetu, monitoring a filtrácia kompletného toku dát medzi nimi, poskytujúcich pokročilú ochranu siete a aplikácií pred škodlivou prevádzkou a hrozbami z internetu.

Bude realizovaná segmentácia siete s určením komunikačných pravidiel pre prestup medzi jednotlivými segmentami siete. Jednotlivé segmenty budú zadefinované na základe analýzy siete a systémov a budú určené komunikačné pravidlá pre prestup medzi jednotlivými segmentami siete. Na segmentáciu siete budú využité súčasné sieťové prepínače a nový firewall.

4.Implementácia log manažmentu

Implementácia centrálneho Log manažment systému pre zber a ukladanie logov z jednotlivých informačných systémov - obstaranie HW s podporou.

Tento cieľ bude naplnený zakúpením a implementáciou zariadenia pre centrálny zber systémových logov z rôznych zariadení a systémov prevádzkovaných v sieti univerzity. Tento systém bude prevádzkovaný na samostatnom hardvérovom zariadení, čo zabezpečí uchovanie logov aj v prípade výpadku primárnej infraštruktúry využívaných na prevádzku univerzitných systémov. Systém bude poskytovať dostatočnú úložnú kapacitu na ukladanie logov.

5. Nezávislý audit kybernetickej bezpečnosti

Pred podaním ŽoNFP (po vyhlásení výzvy) bol vykonaný nezávislý audit kybernetickej bezpečnosti, na základe ktorého boli nastavené aktivity v ŽoNFP, aby sa realizáciou projektu zvýšila KB UK.

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 UK - 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

Univerzita Komenského v Bratislave 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.) takéhoto Informačného systému alebo jeho časti. Zároveň odovzdaný Vytvorený zdrojový kód musí byť pokrytý testami (aspoň na 90%) a dosahovať rating kvality (statická analýza kódu) podľa CodeClimate/CodeQLa pod. (minimálne stupňa B).
- Pre zamedzenie pochybností, povinnosti Zhotoviteľa týkajúce sa Vytvoreného zdrojového kódu platí i na akékoľvek opravy, zmeny, doplnenia, upgrade alebo update Vytvoreného zdrojového kódu a/alebo vyššie uvedenej dokumentácie, ku ktorým dôjde pri plnení tejto Zmluvy o dielo alebo v rámci záručných opráv. Vytvorené zdrojové kódy budú vytvorené vyexportovaním z produkčného prostredia a budú odovzdané Objednávateľovi na elektronickom médiu v zapečatenom obale. Zhotoviteľ je povinný umožniť Objednávateľovi pri odovzdávaní Vytvoreného zdrojového kódu, pred zapečatením obalu, skontrolovať v priestoroch Objednávateľa prítomnosť Vytvoreného zdrojového kódu na odovzdávanom elektronickom médiu.
- Nebezpečenstvo poškodenia zdrojových kódov prechádza na Objednávateľa momentom prevzatia Informačného systému alebo jeho časti, pričom Objednávateľ sa zaväzuje uložiť zdrojové kódy takým spôsobom, aby zamedzil akémukoľvek neoprávnenému prístupu tretej osoby. Momentom platnosti SLA zmluvy umožní Objednávateľ poskytovateľovi, za predpokladu, že to je nevyhnutné, prístup k Vytvorenému zdrojovému kódu výlučne na účely plnenia povinností z uzatvorenej SLA zmluvy.

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

7. Prevádzka a údržba

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 Prevádzkové požiadavky

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	

8. Požiadavky na personál

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

- Predseda RV – prof. JUDr. Marek Števček, DrSc.
- Biznis vlastník – doc. RNDr. Eva Viglašová, PhD.
- Zástupca vlastníkov procesov – Ing. Pavel Beňo, PhD.
- Projektový manažér objednávateľa (PM) – Mgr. Michal Lenhart, PhD.

Projektový tím objednávateľa:

- Manažér kybernetickej bezpečnosti – Ing. Rastislav Kulhánek, PhD.
- Kľúčový používateľ – RNDr. Tomáš Fazekaš, PhD.
- Projektový manažér objednávateľa (PM) – Mgr. Michal Lenhart, PhD.

Všetci členovia tímu sú internými zamestnancami UK ku dňu podania ŽoNFP.

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., 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. , 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: KĽÚČOVÝ POUŽÍVATEĽ (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: 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 opatrenia môžu byť realizované paralelne, dokonca rôznymi tímami, avšak na základe vopred stanovenej stratégie a plánu celého projektu. Agilný prístup na realizáciu nami plánovaného projektu nie je vhodný i s ohľadom na potrebu realizácie projektu za plnej prevádzky základnej služby UK.

10. Prílohy

Dokument neobsahuje prílohy.