projekt_2660_Projektovy_zamer_ramcovy

PROJEKTOVÝ ZÁMER

Vzor pre manažérsky výstup I-02

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, SKRATKY (KONVENCIE) A DEFINÍCIE

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

Dokument Projektový zámer v zmysle vyššie uvedenej vyhlášky a prílohy č. 8 výzvy PSK-MIRRI-614-2024-DV-EFRR (Podpora v oblasti kybernetickej a informačnej bezpečnosti na regionálnej úrovni – verejné a štátne vysoké školy) obsahuje manažérske zhrnutie, motiváciu a rozsah projektu, zainteresované strany, ciele projektu a merateľné ukazovatele, návrh organizačného zabezpečenia projektu, alternatívy, opis obmedzení, predpokladov, tolerancií, opis požadovaných výstupov, náhľad architektúry, opis rozpočtu, detailný popis nákladov a prínosov, postup a spôsob nacenenia projektu, harmonogram projektu a zoznamom rizík a závislostí.

V zmysle usmernenia MIRRI SR sa v projektovej dokumentácii (ani v ŽoNFP) 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. Rovnako sú v zmysle usmernenia MIRRI SR manažérske produkty napísané 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:

Fxx

F – funkčná požiadavka xx – číslo požiadavky

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

Nxx

N – nefukčná požiadavka (NFR) xx – číslo požiadavky

Technické požiadavky majú nasledovnú konvenciu:

Txx

T – technická požiadavka xx – číslo požiadavky

3. DEFINOVANIE PROJEKTU

3.1 Manažérske zhrnutie

Univerzita Komenského v Bratislave (ďalej len „UK") momentálne nie je prevádzkovateľom základnej služby podľa zákona č. 69/2018 Z. z. Zákona o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „ZoKB"), ale predpokladá sa, že s pripravovanou transpozíciou smernice NIS2 do slovenskej legislatívy, bude musieť plniť požiadavky vyplývajúce z tejto legislatívy. UK podporuje zvyšovanie kybernetickej bezpečnosti nielen z legislatívnych dôvodov, ale aj z dôvodu zabezpečenia vlastných prevádzkovaných systémov voči narastajúcim kybernetickým hrozbám. UK si nechala vypracovať audit KB na základe požiadaviek ZoKB, z ktorého vyplynuli nesúlady s požiadavkami zákona.

UK 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.) nespĺňa niektoré požiadavky. Ide primárne o chýbajúcu, resp. neaktuálnu dokumentáciu a o niektoré technologické požiadavky, ktorých zaobstaranie je finančne náročné.

UK chce zvýšiť všeobecnú úroveň kybernetickej bezpečnosti zapojením sa do výzvy a realizovaním nasledovných krokov:

- Zvýšiť súlad s legislatívnymi požiadavkami v týchto oblastiach:
- inventarizácia aktív, klasifikácia informácií a kategorizácia sietí a informačných systémov, spolu s vykonaním analýzy rizík a analýzy dopadov a následným riadením identifikovaných rizík
- vytvorením, resp. aktualizovaním kompletnej bezpečnostnej dokumentácie podľa požiadaviek ZoKB
- personálne zabezpečenie role manažéra kybernetickej bezpečnosti
- zvýšiť sieťovú a komunikačnú bezpečnosť nasadením a implementáciou perimetrového firewallu a zabezpečiť zaškolenie personálu na jeho administráciu a obsluhu
- implementáciu centrálneho log manažment systému pre zber a ukladanie logov zo systémov univerzity
- implementovať do existujúceho manažmentu identít manažment rolí a integráciu čo najviac systémov unverzity s týmto IDM systémom

Ciele projektu

Ciele projektu sú definované v súlade s Národnou koncepciou informatizácie verejnej správy (ďalej len „NKIVS“):

- Zabezpečenie bezpečnosti prevádzky IS a sietí vrátane sieťovej a komunikačnej bezpečnosti
- Zaznamenávanie udalostí a monitorovanie a riešenie KIB incidentov
- Zabezpečenie kontinuity prevádzky

Dané ciele budú dosiahnuté realizáciou hlavnej aktivity projektu - Realizácia opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti.

Cieľová skupina

Cieľovou skupinou sú zamestnanci UK, študenti UK, dodávatelia UK a ostatné právnické osoby využívajúce systémy UK.

Realizáciou aktivít projektu dosiahne UK naplnenie hlavného cieľa, ktorým je zvýšenie informačnej a kybernetickej bezpečnosti a zabezpečenia ochrany údajov a elektronických dát, ktoré sú využívané UK, zamestnancami ako aj študentmi.

Projekt je v súlade s intervenčnou stratégiou Programu Slovensko 2021-2027 v nasledovných oblastiach:

- súlad projektu so špecifickým cieľom: RSO1.2 (opatrenie 1.2.1)
- súlad s očakávanými výsledkami definovanými v Partnerskej dohode pre špecifický cieľ RSO 1.26 3) súlad s definovanými typmi oprávnených aktivít v rámci výzvy.

Realizáciou projektu budú naplnené nasledovné merateľné ukazovatele:

PO095 / PSKPSOI12 – cieľová hodnota 1

PR017 / PSKPRCR11 – cieľová hodnota 84 455

Miesto realizácie:

Univerzita Komenského v Bratislave

Predpokladaný rozpočet projektu (oprávnených výdavkov) je 488 991,28 EUR s DPH.

V prípade, že by mala UK investovať do dobudovania kybernetickej bezpečnosti vlastné finančné prostriedky, je prakticky nereálne zrealizovať všetky povinnosti podľa zákona o kybernetickej bezpečnosti a zákona o informačných systémoch verejnej správy, nakoľko ide o pomerne vysoké náklady v krátkom časovom období.

S ohľadom na to, že univerzity majú limitované finančné zdroje na boj s kyberútokmi, a súčasne je ich povinnosťou dodržiavať ustanovenia zákona o ISVS a s vysokou pravdepodobnosťou bude musieť spĺňať aj požiadavky ZoKB o kybernetickej bezpečnosti, vyhlásilo MIRRI SR Výzvu, ktorá má umožniť aj inštitúciám ako UK získať prostriedky na ochranu informačných systémov a dosiahnutie kybernetickej bezpečnosti na najvyššej úrovni pri minimálnych nákladoch.

Projekt je vypracovaný v súlade s nasledovným typom aktivity:

- Zlepšovanie technologického, procesného, infraštruktúrneho, vedomostného a organizačného zabezpečenia zručností a kapacít pre plnenie úloh v oblasti KIB v prostredí orgánov štátnej a verejnej správy s definovanou hlavnou aktivitou: Realizácia opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti.

Sumarizácia hlavných parametrov hodnotenia predkladaného projektu:

P. č.	Názov hodnotiaceho kritéria	Parametre v projekte	Zdroj
1.	Miera rizík ohrozujúcich úspešnú realizáciu projektu	V rámci projektu bolo identifikovaných menej ako 10 % rizík z celkového počtu identifikovaných rizík v ŽoNFP s vysokou závažnosťou, ktoré ohrozujú úspešnú realizáciu projektu.	Príloha 1 zoznam rizík
2.	Administratívne, odborné a prevádzkové kapacity žiadateľa	Žiadateľ disponuje a plánuje (v súlade s podmienkami výzvy) dostatočné odborné kapacity s náležitou odbornou spôsobilosťou a know-how na riadenie a implementáciu projektu v danej oblasti. Popis zabezpečenia prevádzky riešenia je reálny, t. j. žiadateľ disponuje a plánuje (v súlade s podmienkami výzvy) personálne kapacity pre zabezpečenie prevádzky riešenia.	Informácie o projektovom tíme sú uvedené v PZ.

3.	Miera oprávnenosti výdavkov projektu	Všetky oprávnené aktivity vychádzajú z bodu 2 Výzvy a prílohy č. 8 Výzvy, ktorá definuje oprávnené podaktivity	V rámci projektu budú realizované nasledovné oprávnené podaktivity: 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 činnosti
4.	Dôležitosť kybernetickej bezpečnosti u žiadateľa a potencionálny dopad kybernetických incidentov	V zmysle kapitoly 3.2.5 PODPORA V OBLASTI KIB NA REGIONÁLNEJ ÚROVNI uvedenej v prílohe 2 Výzvy boli Identifikované jednotlivé kategórie.	§ 24 ods. 2 písm. a) – kategória: II § 24 ods. 2 písm. b) a c) – kategória: II § 24 ods. 2 písm. d) – kategória: III §24 ods. 2 písm. e) – kategória: I

3.2 Motivácia a rozsah projektu

Hlavnou motiváciou projektu je zvýšenie úrovne KIB, aby UK bola lepšie pripravená čeliť interným a externým hrozbám v oblasti kybernetickej bezpečnosti. Na rozdiel od súčasného stavu bude disponovať výrazne vyššími schopnosťami detekcie škodlivých aktivít, technologické vybavenie bude umožňovať lepšiu ochranu pred útokmi z externého a interného prostredia, ako aj ochranu dát.

Medzi hlavné ciele systému riadenia KIB patria:

- zabezpečenie správnej a bezpečnej prevádzky prostriedkov spracúvajúcich informácie,
- monitorovanie prostredia,
- evidencia a ošetrovanie podozrivých udalostí a bezpečnostných incidentov s dôrazom na prevenciu ich opakovaného výskytu.

Vyhlásená výzva „Podpora v oblasti kybernetickej a informačnej bezpečnosti na regionálnej úrovni – verejné a štátne vysoké školy" súvisí najmä s naplnením povinností:

- definovanými v zákone č. 69/2018 Z. z. Zákon o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon o KB") a v zákone č. 95/2019 Z. z. Zákon o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ITVS").
- opatreniami definovanými v § 20 zákona o KB.
- nutnosť zvýšenia úrovne a schopnosti zabezpečovať a riadiť informačnú a kybernetickú bezpečnosť vzhľadom na sústavne sa zvyšujúce hrozby a riziká,
- zabezpečenie realizácie spoločných blokov bezpečnostnej architektúry v súlade s NKIVS a strategickou prioritou informačnej a kybernetickej bezpečnosti,
- ako reakcia na aktuálny nedostatočný stav úrovne vyspelosti procesov riadenia KIB,
- ako reakcia na aktuálne zmeny v používaní IT, ako aj závažné útoky v oblasti kybernetickej bezpečnosti

Implementácia projektu bude prebiehať v nasledovných krokoch:

Hlavná aktivita: Realizácia opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti

1. Prípravná fáza a Iniciačná fáza
2. Realizačná fáza

2a Analýza a Dizajn

2b Nákup technických prostriedkov, programových prostriedkov a služieb

2c Implementácia a testovanie

2d Nasadenie opatrení

1. Dokončovacia fáza
2. Podpora prevádzky (SLA)

Podporné aktivity – nepriame výdavky

- Podporná aktivita – Projektový manažér interný/externý na riadenie hlavných aktivít projektu.
- Podporná aktivita – Publicita a informovanosť v zmysle manuálu

Súčasné bezpečnostné mechanizmy v oblasti monitoringu a hodnotenia zraniteľnosti implementované univerzitou tvoria základ, ktorý si vyžaduje ďalší rozvoj pre zaistenie primeranej ochrany spracúvaných informácií voči kybernetickým hrozbám a zároveň zabezpečenie súladu s povinnosťami vyplývajúcimi z ustanovení zákona č.69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Okrem legislatívnych požiadaviek je nevyhnutné brať do úvahy aj aktuálny stav, ktorá je z časti spôsobený neschopnosťou včasnej detekcie možného kybernetického útoku z dôvodu absentujúcich bezpečnostných opatrení, chýbajúcich analytických nástrojov a nedostatku kvalitných zdrojov bezpečnostne relevantných záznamov.

3.2.1 Hlavný popis problému

UK v Bratislave momentálne nespadá pod Zákon o kybernetickej bezpečnosti (ďalej len ZoKB), ale s pripravovanou transpozíciou smernice NIS2 do slovenskej legislatívy bude musieť plniť požiadavky z tejto legislatívy vyplývajúce. UK si nechala vypracovať audit KB univerzity na základe požiadaviek ZoKB, z ktorého vyplynuli nesúlady s požiadavkami zákona. UK si samozrejme uvedomuje potrebu zvyšovania kybernetickej bezpečnosti nielen z legislatívnych dôvodov, ale aj z dôvodu zabezpečenia vlastných prevádzkovaných systémov voči narastajúcim kybernetickým hrozbám..

UK 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.) nespĺňa niektoré požiadavky. Ide primárne o chýbajúcu, resp. neaktuálnu dokumentáciu a o niektoré technologické požiadavky, ktorých zaobstaranie je finančne náročné.

UK plánovaným zapojením do projektu chce zvýšiť všeobecnú úroveň kybernetickej bezpečnosti realizovaním nasledovných krokov:

- vypracovanie alebo aktualizácia bezpečnostnej dokumentácie vrátane rozsahu a spôsobu plnenia všeobecných bezpečnostných opatrení,
- vypracovanie a implementácia špecifických interných riadiacich aktov pre vybrané oblasti kybernetickej a informačnej bezpečnosti,
- vypracovanie štatútu bezpečnostného výboru,
- vypracovanie bezpečnostného projektu informačného systému verejnej správy,
- identifikácia všetkých 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 a implementácia 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 a implementácia postupov a procesov upravujúcich personálnu bezpečnosť organizácie prostredníctvom interného riadiaceho aktu,
- vypracovanie a implementácia 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 a implementácia 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;
- 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;
- implementácia centrálneho Log manažment systému pre zber a ukladanie logov z jednotlivých informačných systémov;

- 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;
- obstaranie prvého alebo opakovaného auditu kybernetickej bezpečnosti v súlade so zákonom o KB;

Na základe zistení z vykonaného auditu je možné vyjadriť, že súčasná implementácia bezpečnostných opatrení je na 11% v súlade so zákonnými požiadavkami.

Hlavné zistenia auditu sú nasledovné:

- Informačné systémy sú prevádzkované spôsobom, ktorý síce zabezpečuje ich dostupnosť, ale v zásade bez akejkoľvek bezpečnosti. Bezpečnosť sa rieši ako splnenie administratívnej povinnosti namiesto toho, aby bola integrálnou súčasťou dizajnu a prevádzky systémov.
- Ako bezpečnostný princíp sa uplatňuje „security by obscurity“ – informácie sa zámerne nezdieľajú, aby sa predišlo ich zneužitiu. Tento princíp bol už veľa krát vyvrátený a preukázateľne znižuje bezpečnosť.
- Dokumentácia (bezpečnostná aj prevádzková) je buď neaktuálna, neexistuje, alebo o nej nikto nevie (súvisí aj s princípom „security by obscurity “). Tým pádom nie je reálne možné riešiť zastupiteľnosť, ani personálnu bezpečnosť.
- Až na malé výnimky neexistujú žiadne prevádzkové ani bezpečnostné smernice.
- Väčšina systémov a aplikácií nie je pravidelne aktualizovaná.
- Chýba väčšina odporúčaných technických opatrení, s výnimkou antivírovej ochrany a dobrej úrovne správy používateľských identít, vrátane Active Directory domény.

Napriek tomu, že výsledok auditu nevyzerá priaznivo, je nutné podotknúť, že z dôvodu povahy auditu sú uvádzané iba nesúlady. Je viacero oblastí, kde je implementácia opatrení na vysokej úrovni. Celkovo je možné konštatovať, že IT je na univerzite prevádzkované tak, aby IT fungovalo s čo najmenším rozpočtom v dobrej viere, že nenastane bezpečnostný incident. Takýto incident má potenciál spustiť kaskádu problémov.

S ohľadom na vyššie uvedené bude teda predmetom projektu riešenie problematiky z nasledovných oprávnených oblastí podľa výzvy:

- 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 činnosti

Hlavným problémom, ktorému UK čelí je teda vyriešenie vyššie pomenovaných oblastí informačnej a kybernetickej bezpečnosti tak, aby bol dosiahnutý významný pokrok pri plnení súladu v oblasti príslušných predpisov KIB a súčasne aby boli technologické náležitosti KIB realizované tak, aby:

- chránili IT systémy a siete, ktoré zabezpečujú prevádzku služieb univerzity pred kybernetickými útokmi,
- plnili svoje úlohy počas implementácie i v čase udržateľnosti projektu,
- boli pripravené na ďalší rozvoj IT technológií a služieb poskytovaných univerzitou,
- bolo možné ich flexibilne rozširovať bez ohrozenia prevádzkovaných i budúcich IT systémov,
- bolo možné nasadenie definovaných procesov stratégie kybernetickej bezpečnosti a bezpečnostných politík.

3.2.2 Biznis procesy

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

- Organizácia bezpečnosti
- Riadenie bezpečnostných rizík

- Riadenie informačných aktív
- Pravidlá správania a dobrej praxe
- Riadenie dodávateľských vzťahov
- Riadenie údržby v oblasti informačno-komunikačných technológií
- Riadenie a prevádzka informačno-komunikačných technológií
- Riadenie súladu
- Riadenie kontinuity procesov a činností

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

3.2.3 Oblasti zamerania projektu

Projekt sa primárne zaoberá oblasťou zabezpečenia opatrení KIB v zmysle zákona o kybernetickej bezpečnosti a zákona o ISVS. Ako bude uvedené ďalej, tento projekt má priamy dopad na všetky ISVS a technologické platformy, ktoré sú určené na poskytovanie služieb univerzity UK, nakoľko výsledky projektu budú ochraňovať všetky IS pred potenciálnymi hrozbami kybernetickej a informačnej bezpečnosti.

3.2.4 Rozsah projektu

Realizácia projektu sa dotkne nasledovných ISVS prevádzkovaných na úrovni UK:

- isvs_14301 - Kamerový systém
- isvs_10452 - Webový portál Univerzity Komenského
- isvs_14300 - Systém pre správu identít
- isvs_14298 - e-learning
- isvs_14297 - Akademický informačný systém

Realizácia projektu sa dotkne nasledovných subjektov:

- Univerzita Komenského v Bratislave
- Interní zamestnanci univerzity
- Externí zamestnanci univerzity
- Študenti
- Podnikatelia - dodávateľsko-odberateľské vzťahy

3.2.5 Motivácia a obmedzenia pre dosiahnutie cieľov projektu

Hlavnou motiváciou je realizácia opatrení KIB definovaných v zákone o kybernetickej bezpečnosti a v zákone o ISVS. Primárne ide o tie opatrenia, ktoré vykazujú najväčší nesúlad s uvedenými právnymi normami a vyhláškou 362/2018 Z. z.. Vďaka realizácii týchto opatrení budú IS UK chránené v maximálnej možnej miere pred kybernetickým incidentom, ktorý by mohol mať na poskytovanie služieb a prevádzku IS UK nasledovný dopad:

Dopad kybernetického bezpečnostného incidentu v závislosti	**Kategória**	**Vysvetlenie**
§ 24 ods. 2 písm. a) zákona 69/2018 Z.z. Počet používateľov základnej služby zasiahnutých kybernetickým bezpečnostným incidentom.	II.	UK disponuje systémami, ktorých výpadok zasiahne viac ako 50 000 užívateľov univerzity. To znamená študentov, zamestnancov a externých partnerov.

§ 24 ods. 2 písm. b) zákona 69/2018 Z.z. Dĺžka trvania kybernetického bezpečnostného incidentu (čas pôsobenia kybernetického bezpečnostného incidentu) a/alebo § 24 ods. 2 písm. c) zákona Geografické rozšírenie kybernetického bezpečnostného incidentu.	II.	UK prevádzkuje systémy pre interný personál, vedeckých pracovníkov a študentov, kde škoda, ktorá nastane je v rozsahu nad 50 000 používateľov.
§ 24 ods. 2 písm. d) zákona 69/2018 Z.z. Stupeň narušenia fungovania základnej služby.	III.	V prípade nefunkčnosti informačných systémov nie je k dispozícii náhradné riešenie.
§ 24 ods. 2 písm. e) zákona 69/2018 Z.z. Rozsah vplyvu kybernetického bezpečnostného incidentu na hospodárske alebo spoločenské činnosti štátu	I.	Incident spôsobí škody, ktoré má/môže mať dopad na viac ako 50 000 osôb. V prípade napadnutia a uniku osobných dát, informáciách o postavení, platových podmienkach a krádeže know how a vedeckých výskumov, by boli škody veľmi veľké a možno aj fatálne. Nefunkčnosť systémov má priamy vplyv na hospodárske alebo spoločenské činnosti. Nefunkčnosť ISVS má priamy súvis na finančné operácie medzi univerzitou a dodávateľmi, odberateľmi, štátnymi inštitúciami (napr. sociálne a zdravotné poisťovne, daňový úrad...). Úspešný kybernetický útok, ktorého cieľom by bolo získanie dát z univerzity môže viesť a pravdepodobne aj bude viesť k úniku osobných údajov a následnému porušeniu práv dotknutých osôb. Vzhľadom na znenie §104 zákona č.: 18/2018 Z. z. a obdobné sankcie uvedené v GDPR môže vzniknúť škoda univerzite až do výšky 20 mil. €. Vychádzajúc z praxe a známych prípadov porušenia zákona na ochranu osobných údajov na území Slovenska môže takto jednému užívateľovi ISVS vzniknúť škoda prevyšujúca 250 000 €.

Projekt je formulovaný tak, aby po jeho realizácii nastal čo najväčší súlad zabezpečenia kybernetickej a informačnej bezpečnosti so zákonom o kybernetickej bezpečnosti a so zákonom o ISVS.

Obmedzenia projektu:

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

3.3 Zainteresované strany/Stakeholder

ID	AKTÉR / STAKEHOLDER	SUBJEKT (názov / skratka)	ROLA (vlastník procesu/ vlastník dát/zákazník/ užívateľ …. člen tímu atď.)	Informačný systém (MetaIS kód a názov ISVS)
1.	Univerzita - Administrátor IT	Uni	Vlastník procesu/ vlastník dát/ prevádzkovateľ / Užívateľ IS Zabezpečuje prevádzku IT	isvs_14301 - Kamerový systém isvs_10452 - Webový portál Univerzity Komenského isvs_14300 - Systém pre správu identít isvs_14298 - e-learning isvs_14297 - Akademický informačný systém

2	Manažér kybernetickej bezpečnosti	Uni	Zodpovedný za KIB	isvs_14301 - Kamerový systém isvs_10452 - Webový portál Univerzity Komenského isvs_14300 - Systém pre správu identít isvs_14298 - e-learning isvs_14297 - Akademický informačný systém
3.	Zamestnanec	Uni	Využíva IS Uni	isvs_14301 - Kamerový systém isvs_10452 - Webový portál Univerzity Komenského isvs_14300 - Systém pre správu identít isvs_14298 - e-learning isvs_14297 - Akademický informačný systém
4.	Študent	Uni	Využíva IS Uni	isvs_14301 - Kamerový systém isvs_10452 - Webový portál Univerzity Komenského isvs_14300 - Systém pre správu identít isvs_14298 - e-learning isvs_14297 - Akademický informačný systém
5.	podnikateľ		Využíva služby prostredníctvom IS	isvs_14301 - Kamerový systém isvs_10452 - Webový portál Univerzity Komenského isvs_14300 - Systém pre správu identít isvs_14298 - e-learning isvs_14297 - Akademický informačný systém
6.	Poskytovateľ IT služieb		Poskytuje služby IS	isvs_14301 - Kamerový systém isvs_10452 - Webový portál Univerzity Komenského isvs_14300 - Systém pre správu identít isvs_14298 - e-learning isvs_14297 - Akademický informačný systém

3.4 Ciele projektu

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

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

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

Cieľ 4.1 Zvýšenie schopnosti včasnej identifikácie kybernetických incidentov vo verejnej správe

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

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

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

4.1 Dôveryhodný štát pripravený na hrozby.

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

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

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

Hlavným cieľom je do prostredia univerzity zaviesť optimalizáciu procesov riadenia kybernetickej bezpečnosti, riadenie rizík, kontinuity činností a riadenie incidentov pomocou finančných prostriedkov z dopytovej výzvy „Podpora v oblasti kybernetickej a informačnej bezpečnosti na regionálnej úrovni – verejné a štátne vysoké školy“. Po implementácii projektu bude proces zavedený a ďalej vykonávaný aj internými zamestnancami, predovšetkým manažérom kybernetickej bezpečnosti, manažérom informačnej bezpečnosti a ďalšími bezpečnostnými zamestnancami. Hlavným výsledkom realizácie projektu bude realizácia a optimalizácia procesov riadenia kybernetickej bezpečnosti, riadenia rizík, kontinuity činností a riadenia incidentov.

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

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

* Definícia strategického cieľa vychádza zo strategického cieľa v Národnej stratégii kybernetickej bezpečnosti a nadväzuje na prioritný cieľ Národnej koncepcie informatizácie verejnej správy.

3.5 Merateľné ukazovatele (KPI)

ID	ID /Názov cieľa	Názov ukazovateľa (KPI)	Popis ukazovateľa	Merná jednotka	AS IS merateľné hodnoty (aktuálne)	TO BE Merateľné hodnoty (cieľové hodnoty)	Spôsob ich merania	Pozn.
1	PO 095 / PS KPS OI12	Verejné inštitúcie podporované v rozvoji kybernetických služieb, produktov a procesov	Počet verejných inštitúcií, ktoré sú podporované za účelom rozvoja a modernizácie kybernetických služieb, produktov, procesov a zvyšovania vedomostnej úrovne napríklad v kontexte opatrení smerujúcich k elektronickej bezpečnosti verejnej správy.	Verejné inštitúcie	0	1	Identifikácia počtu realizácie opatrení KIB pre inštitúciu – splnenie súladu KIB so zákonom o kybernetickej bezpečnosti a zákonom o ISVS Čas plnenia merateľného ukazovateľa projektu: Fyzické ukončenie realizácie hlavných aktivít projektu	Typ ukazovateľa: Výstup

	PR 017 / PS KPR CR 11	Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov	Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov	Uží vate lia / rok	0	844 55	Sumarizácia počtu používateľov nových a vylepšených digitálnych služieb – bude určené počtom prístupov v IAM, Databázou používateľov v oblasti KIB. V prípade univerzity ide o počet používateľov, ktorí priamo využívajú IS a priamo sa podieľajú na zabezpečovaní základnej služby. Čas plnenia merateľného ukazovateľa projektu: v rámci udržateľnosti projektu	Typ uk az ov at eľ a: vý sle dok

3.5.1 Špecifikácia potrieb koncového používateľa

Z pohľadu UK je koncovým používateľom IT oddelenie a sekundárne zamestnanci UK a študenti, ktorí očakávajú, že nebude vplyvom kybernetických útokov dochádzať k výpadkom prevádzky IS univerzity a tým sa de facto znefunkční poskytovanie univerzitných služieb.

Univerzita Komenského v Bratislave momentálne nespadá pod Zákon o kybernetickej bezpečnosti (ďalej len ZoKB), ale s pripravovanou transpozíciou smernice NIS2 do slovenskej legislatívy bude musieť plniť požiadavky z tejto legislatívy vyplývajúce. UK si nechala vypracovať audit KB na základe požiadaviek ZoKB, z ktorého vyplynuli nesúlady s požiadavkami zákona. UK si samozrejme uvedomuje potrebu zvyšovania kybernetickej bezpečnosti nielen z legislatívnych dôvodov, ale aj z dôvodu zabezpečenia vlastných prevádzkovaných systémov voči narastajúcim kybernetickým hrozbám.

UK 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.) nespĺňa niektoré požiadavky. Ide primárne o chýbajúcu, resp. neaktuálnu dokumentáciu a o niektoré technologické požiadavky, ktorých zaobstaranie je finančne náročné.

UK plánovaným zapojením do projektu chce zvýšiť všeobecnú úroveň kybernetickej bezpečnosti realizovaním krokov popísaných v časti 3.2.1 Hlavný popis problému, pomocou nasledovných aktivít **– predmet plnenia:**

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.

3.6 Riziká a závislosti

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

3.7 Stanovenie alternatív v biznisovej vrstve architektúry

Posudzovanie alternatív riešenia vychádza z viacerých možností. Prichádzajú do úvahy nasledovné 3 alternatívy:

1. Ponechanie existujúceho stavu – ide o nultý stav, v ktorom UK nespĺňa požiadavky na kybernetickú bezpečnosť a ide o možné ohrozenie informačných systémov.
2. Realizácia projektu KIB s doplnením vybraných opatrení (t.j. nie všetkých tu navrhnutých) – došlo by k zvýšeniu súladu s legislatívou a s požiadavkami na technické zabezpečenie KB, ale informačné systémy univerzity by boli naďalej ohrozené.
3. Realizácia opatrení na dosiahnutie zvýšenia súladu KIB s požiadavkami zákona o kybernetickej bezpečnosti a zákona o ISVS – pôjde o také zvýšenie súladu s požiadavkami príslušnej legislatívy v oblasti KIB, ktorá zabezpečí ochranu UK pred najväčšími hrozbami.

Z hľadiska identifikovaných procesov v kapitole 3.2.2 alternatíva 1 nepokryje riešenie žiadneho z identifikovaného problémov. V prípade čiastkového riešenia (alternatíva 2) by boli zvolené iba niektoré z procesov, ktoré by boli projektom vyriešené. V prípade alternatívy 3 budú podporené procesy v oblasti KIB, ktoré je potrebné pre účely ochrany IS, a ktoré zabezpečujú prevádzku UK.

Na základe zhodnotenia sa ukazuje ako najprijateľnejšia alternatíva možnosť 3, kedy dôjde k značnému zvýšeniu stavu KB na univerzite a nebude ohrozená udržateľnosť z dôvodu finančnej náročnosti.

3.8 Multikriteriálna analýza

Multikriteriálna analýza je v tomto prípade redukovaná na dva parametre:

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

Z vyššie uvedených možných alternatív vyplýva, že s ohľadom na potreby a finančné možnosti UK v rámci udržateľnosti je najvýhodnejšia a dlhodobo udržateľná alternatíva 3.

3.9 Stanovenie alternatív v aplikačnej vrstve architektúry

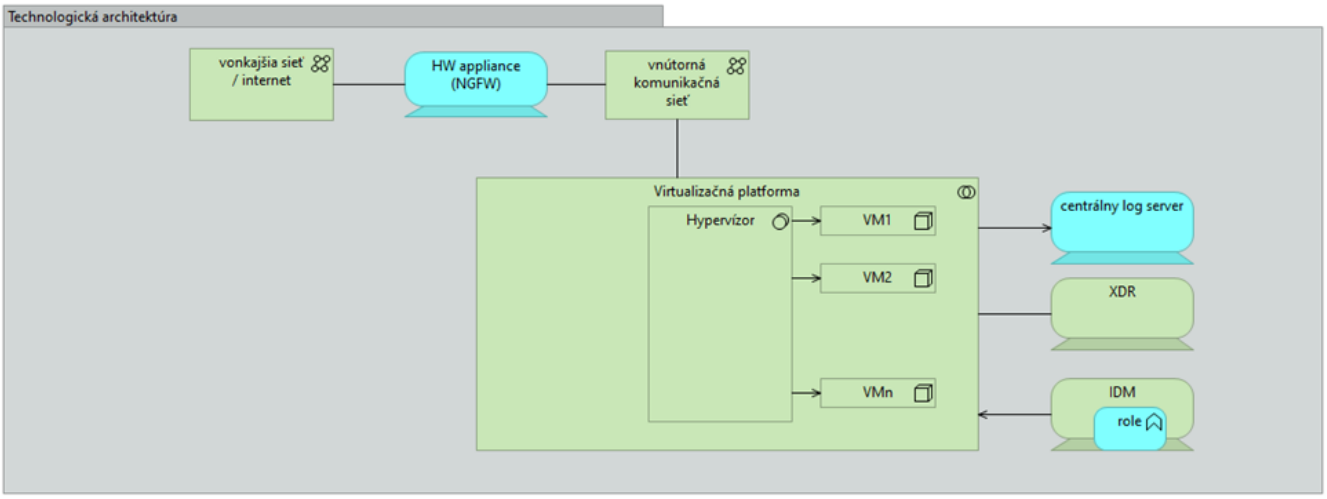
HW a SW komponenty, rovnako ako služby, ktoré sú s nimi spojené musia zodpovedať požiadavkám definovaným v projekte koncovými používateľmi - tými sú v tomto prípade oddelenie informatiky, ktoré vychádza z požiadaviek zákona o kybernetickej bezpečnosti, zákona o ISVS, vyhlášky 362/2018 Z. z. a ďalších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

Z hľadiska aplikácie nie sú definované alternatívy. Aplikačne teda bude zvolená nasledovná architektúra – viď. časť 5 Náhľad architektúry.

3.10 Stanovenie alternatív v technologickej vrstve architektúry

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

Technologickú architektúru riešenia definuje nasledovný obrázok:



4. POŽADOVANÉ VÝSTUPY (PRODUKT PROJEKTU)

Výsledkom projektu budú:

Projektové výstupy v zmysle vyhlášky 401/2023 o riadení projektov. V prípade, že predmetom realizácie bude dielo (oceniteľné práva a/alebo zdrojový kód), získa UK právo vykonávať autorské práva k tomuto dielu, vrátane výhradnej a územne neobmedzenej licencie. Tieto podmienky sa nevzťahujú na tzv. krabicový softvér, ktorý je predávaný ako produkt či už realizátora alebo tretej strany.

Z hľadiska plnenia cieľov projektu bude výsledkom projektu naplnenie hlavného cieľa, t.j. súlad KIB so zákonom o kybernetickej bezpečnosti a so zákonom o ISVS, čo bude naplnené realizáciu nasledovných partikulárnych cieľov:

- 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 činnosti

- Technologicky a administratívne pôjde o realizáciu nasledovných cieľov:

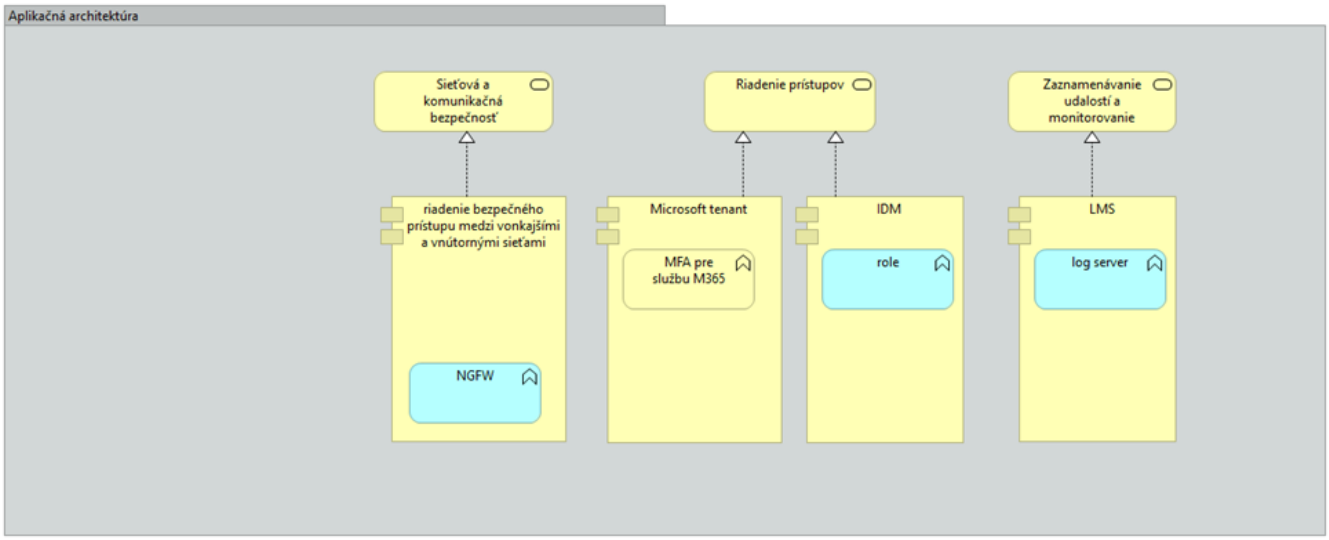
- vypracovanie alebo aktualizácia bezpečnostnej dokumentácie vrátane rozsahu a spôsobu plnenia všeobecných bezpečnostných opatrení,
- vypracovanie a implementácia špecifických interných riadiacich aktov pre vybrané oblasti kybernetickej a informačnej bezpečnosti,
- vypracovanie štatútu bezpečnostného výboru,
- vypracovanie bezpečnostného projektu informačného systému verejnej správy,
- identifikácia všetkých 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 a implementácia 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 a implementácia postupov a procesov upravujúcich personálnu bezpečnosť organizácie prostredníctvom interného riadiaceho aktu,
- vypracovanie a implementácia 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 a implementácia 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;
- 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;
- implementácia centrálneho Log manažment systému pre zber a ukladanie logov z jednotlivých informačných systémov;
- 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;
- obstaranie prvého alebo opakovaného auditu kybernetickej bezpečnosti v súlade so zákonom o KB;

5. NÁHĽAD ARCHITEKTÚRY

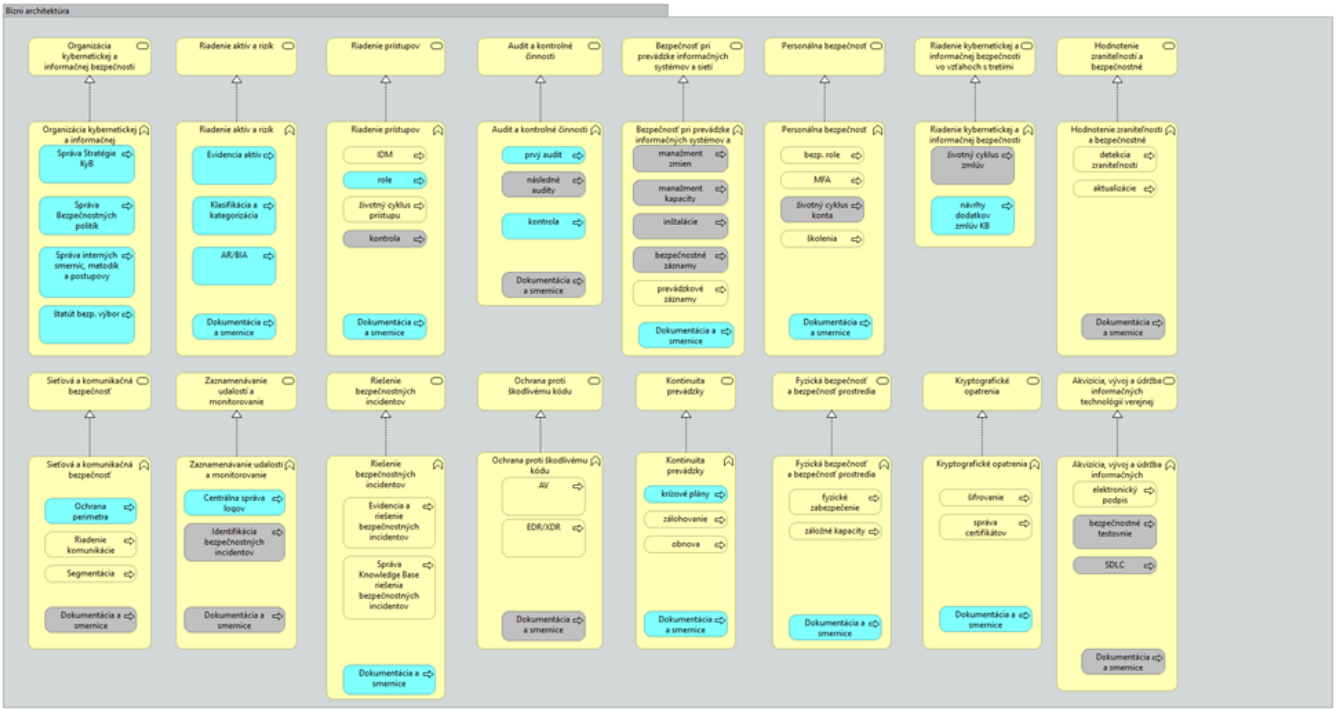
Architektúra celého riešenia je v zmysle usmernenia MIRRI SR rámcová tak, aby bolo z projektu zrejmé, ktoré komponenty v rámci realizácie projektu budú vytvorené (a budú realizovať opatrenia KIB).

Primárne opatrenia kybernetickej bezpečnosti chránia IS UK, ktoré sú určené na prevádzkovanie univerzitných služieb UK. Z vyššie definovaných potrieb je zrejmé, o aké komponenty zabezpečenia pôjde - firewall, centrálny logovací nástroj, 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, kompletná dokumentácia podľa ZoKB vrátane BCM plánov.

Aplikačnú architektúru riešenia definuje nasledovný obrázok:



Biznis architektúra riešenia definuje nasledovný obrázok:



6. LEGISLATÍVA

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

- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
- Vyhláška č.78/2020 Z.z. o štandardoch pre ITVS
- Vyhláška č.401/2023 Z.z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy
- Vyhláška 179/2020 Z.z. o obsahu bezpečnostných opatrení ITVS
- Vyhláška 362/2018 Z.z. o obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení)

7. HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU a METÓDA JEHO RIADENIA

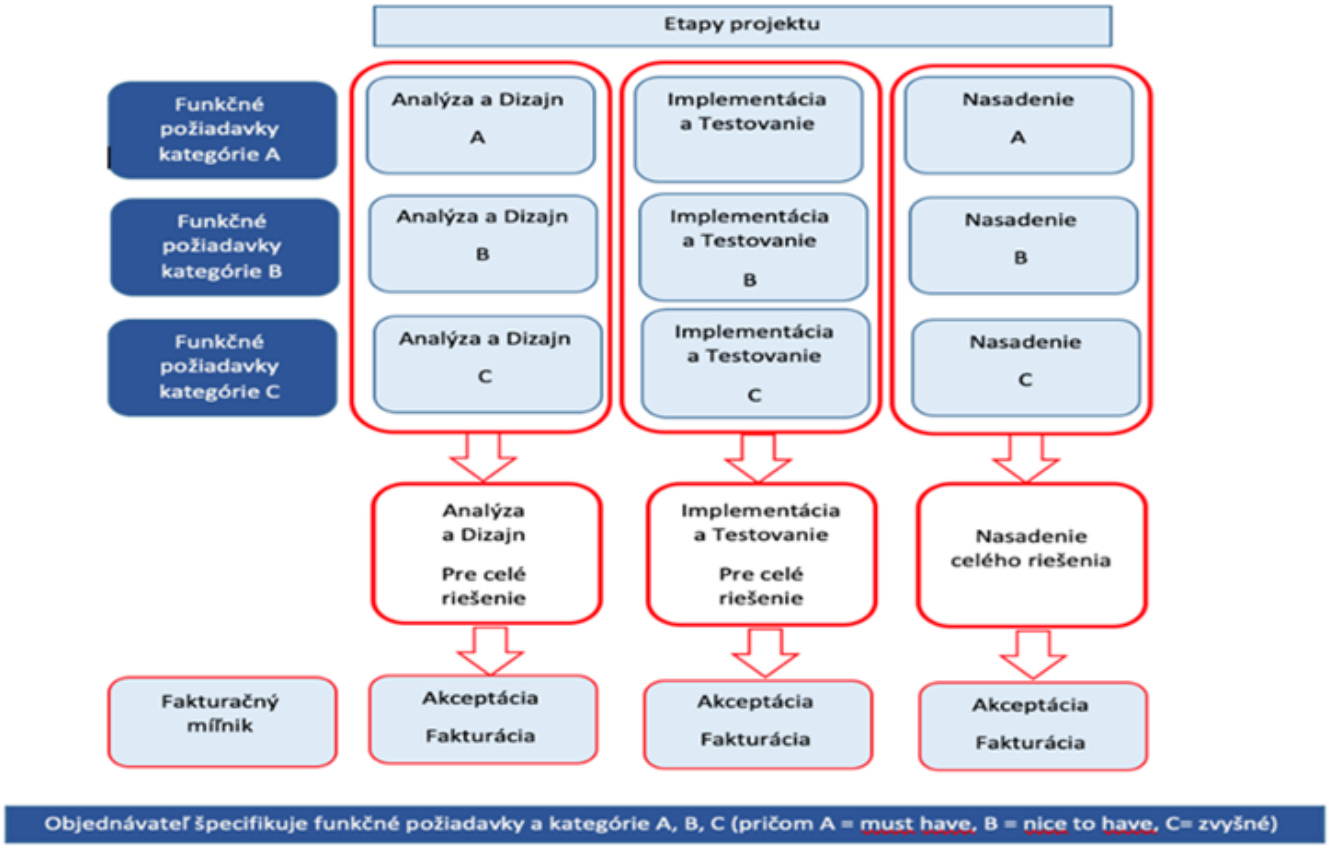
Harmonogram projektu je definovaný na základe odporúčania MIRRI SR, ktoré predpokladá trvanie projektu na úrovni približne jedného roka. S ohľadom na potreby nákupu a implementácie technológií vrátane potreby ich skúšobnej prevádzky sa s týmto časom stotožňujeme.

Začiatok realizačnej fázy projektu vyplýva z predpokladu, že realizácia projektu začne až po ukončení administratívneho a odborného hodnotenia a po podpise Zmluvy o NFP, pričom je definovaná dostatočná časová rezerva na tieto úkony. Rovnako na procesy verejného obstarávania, ktoré môžu potenciálne začať v krátkom čase po podaní žiadosti o NFP.

ID	FÁZA/AKTIVITA	ZAČIATOK (odhad termínu)	KONIEC (odhad termínu)	POZNÁMKA
1.	Prípravná fáza a Iniciačná fáza	4/2024	12 /2024	Podpísanie zmluvy o NFP Spustenie procesov VO
2.	Realizačná fáza	01 /2025	11 /2025	Podpísanie zmlúv s dodávateľmi po ukončení VO, realizácia
2a	Analýza a Dizajn	04 /2025	05 /2025	
2b	Nákup technických prostriedkov, programových prostriedkov a služieb	04 /2025	08 /2025	
2c	Implementácia a testovanie	08 /2025	10/2025	Min. 2 mesiace test. prevádzky
2d	Nasadenie opatrení	10 /2025	11/2025	
3.	Dokončovacia fáza	10/2025	12/2025	Počas dokončovacej fázy projektový manažér pripraví podklady a odovzdá na schválenie záverečnú žiadosť o platbu a záverečnú monitorovaciu správu.
4.	Podpora prevádzky (SLA)	01/2026	01/2031	Obdobie udržateľnosti

Ako metóda riadenia projektu bude použitá metóda „Waterall“. Táto metóda sa ukázala byť ako najvhodnejšia nakoľko svojimi charakteristikami a možnosťami plne zodpovedá požiadavkám a predstavám univerzity.

Schéma metódy projektového riadenia:



8. ROZPOČET A PRÍNOSY

V uvedenom projekte vychádzame pri stanovení rozpočtu z prieskumu trhu a pravidiel stanovených výzvou. S ohľadom na rozpočet projektu (projekt do 1 000 000,00,- EUR) nebola spracovaná Analýza nákladov a prínosov.

8.1 Sumarizácia nákladov a prínosov

Náklady	**Infraštruktúra pre prevádzku kybernetickej bezpečnosti**	**Dokumentácia KB**	**Pre všetky podaktivity:**
IT - CAPEX			
Aplikácie			
SW	25 200,00 €		
HW	115 896,00 €		
Práce/služby	250 505,20 €	62 400,00 €	
Mzdy interní zamestnanci			3 000,00 €
Paušálne výdavky			
IT - OPEX- prevádzka			
Aplikácie			
SW	25 200,00 €		
HW			

8.2 Sumarizácia podľa podaktivít:

Názov	**HW**	**SW**	**Služby**

1.Vytvorenie, resp. aktualizácia kompletnej bezpečnostnej dokumentácie podľa požiadaviek ZoKB Prílohy č. 1 k vyhláške č. 362 /2018 Z. z.			55 200,00 €
2. Zvyšovanie bezpečnosti zamestnancov pomocou nasadenia manažmentu rolí v centrálnom IDM riešení			235 764,00 €
3. implementácia firewall-u	76 800,00 €	25 200,00 €	14 741,20 €
4.Implementácia log manažmentu	39 096,00 €		
5. Audit			7 200,00 €

V prípade projektov kybernetickej bezpečnosti je priame vyčíslenie návratnosti pomerne komplikované. Z pohľadu návratnosti je potrebné venovať sa hodnoteniu možných škôd, ktoré by vznikli v prípade, že nebude adekvátne riešená KIB na úrovni poskytovateľa základnej služby. Ide o nasledovné potenciálne škody:

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

Reputačné riziko – vzhľadom na postavenie a oblasť spoločenskej dôležitosti a zákonných povinností univerzity, je toto riziko potenciálne vysoké – teda v prípade neplnenia legislatívnych požiadaviek v zmysle zákona o kybernetickej bezpečnosti a zákona o ISVS alebo vyhlášky 362 /2018 Z. z. či reálneho výpadku prevádzky základnej služby, úniku citlivých dát v kombinácii aj s prípadnou medializáciou a pod.

9. PROJEKTOVÝ TÍM

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.

ID	Meno a Priezvisko	Pozícia	Oddelenie	Rola v projekte
1.	Mgr. Michal Lenhart	PM	CIT UK	Projektový manažér
2.	Ing. Rastislav Kulhánek, PhD.	PM, MIB	CIT UK	Manažér kybernetickej bezpečnosti

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

10. PRÍLOHY

Príloha : 1- Zoznam rizík a závislostí