PRÍSTUP K PROJEKTU

pre manažérsky výstup I-03

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

Povinná osoba	*Univerzita Pavla Jozefa Šafárika v Košiciach (UPJŠ v Košiciach)*
Názov projektu	Kybernetická a informačná bezpečnosť na UPJŠ v Košiciach
Zodpovedná osoba za projekt	*doc. RNDr. JUDr. Pavol Sokol, PhD.*
Realizátor projektu	*UPJŠ v Košiciach*
Vlastník projektu	*UPJŠ v Košiciach*

Schvaľovanie dokumentu

Položka	**Meno a priezvisko**	**Organizácia**	**Pracovná pozícia**	**Dátum**	**Podpis** (alebo elektronický súhlas)
Vypracoval	doc. RNDr. JUDr. Pavol Sokol, PhD.	UPJŠ v Košiciach	Vedúci úseku informačnej a kybernetickej bezpečnosti	31.5.2024	

1. HISTÓRIA DOKUMENTU

Verzia	**Dátum**	**Zmeny**	**Meno**
0.1	20.05.2024	Pracovný návrh	Pavol Sokol
1.0	31.05.2024	Finálna verzia v súlade so žiadosťou o NFP	Pavol Sokol

2. ÚČEL DOKUMENTU

V súlade s Vyhláškou MIRRI č. 401/2023 Z. z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy (ďalej len „Vyhláška o riadení projektov“) 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 Vyhlášky o riadení projektov 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) obsahovať opis navrhovaného riešenia, architektúru riešenia projektu na úrovni biznis vrstvy, aplikačnej vrstvy, dátovej vrstvy, technologickej vrstvy, infraštruktúry navrhovaného riešenia, bezpečnostnej architektúry, špecifikáciu údajov spracovaných v projekte, čistenie údajov, prevádzku a údržbu výstupov projektu, prevádzkové požiadavky, požiadavky na zdrojové kódy. Dodávané riešenie musí byť v súlade so zákonom. Zároveň opisuje aj implementáciu projektu a preberanie výstupov projektu.

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:

1) **funkčné (používateľské) požiadavky** majú nasledovnú konvenciu:
   Fxx (F – funkčná požiadavka, xx – číslo požiadavky)

2) **Nefunkčné (kvalitatívne, výkonové - Non Functional Requirements - NFR) požiadavky** majú nasledovnú konvenciu:
   Nxx (N – nefukčná požiadavka (NFR), xx – číslo požiadavky)

3) **Technické požiadavky** majú nasledovnú konvenciu:
   Txx (T – technická požiadavka, xx – číslo požiadavky)

3. POPIS NAVRHOVANÉHO RIEŠENIA

Cieľom predloženého projektu je vzhľadom na bezpečnostné hrozby a ich vývoj a súčasne vývoj legislatívnych požiadaviek, **zvýšenie úrovne a odolnosti kybernetickej a informačnej bezpečnosti, najmä kritickej infraštruktúry v prostredí UPJŠ**. Súčasne je cieľom projektu zvýšenie schopnosti UPJŠ identifikovať relevantné bezpečnostné udalosti a následne aj kybernetické bezpečnostné incidenty.

Na splnenie tohto cieľa, bude žiadateľ (UPJŠ) v rámci projektu realizovať opatrenia na zvýšenie úrovne informačnej a kybernetickej bezpečnosti na UPJŠ (ďalej len ako „hlavná aktivita projektu"). Prínosy z tohto projektu budú mať nielen zamestnanci a študenti UPJŠ, ale aj iní používatelia informačných systémov a iných technológií a produktov UPJŠ vrátane používateľov akademického informačného systému AiS2. Vzhľadom na rozsah a komplexnosť riadenia informačnej a kybernetickej bezpečnosti, ako aj povahu jednotlivých bezpečnostných opatrení, projekt je rozdelený do niekoľkých podaktivít (čiastkových úloh):

(A) Riadenie informačnej a kybernetickej bezpečnosti

V rámci projektu dôjde k vypracovaniu, resp. doplneniu dokumentácie nevyhnutnej k riadeniu informačnej a kybernetickej bezpečnosti na UPJŠ. Súčasťou projektu bude vypracovanie bezpečnostnej stratégie a bezpečnostnej politiky a doplnenie inventarizácie aktív, analýzy aktív, bezpečnostných hrozieb, zraniteľností, rizík a dopadov. Pre každú oblasť bezpečnostných opatrení uvedených vo vyhláške NBÚ č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška NBU") dôjde k spracovaniu nevyhnutnej dokumentácie a nastaveniu príslušných procesov. Dôjde k realizácii nasledujúcich podaktivít (činností):

1) Vypracovanie a aktualizácia bezpečnostnej dokumentácie
   - vypracovanie a implementácia špecifických interných riadiacich aktov pre vybrané oblasti kybernetickej a informačnej bezpečnosti,
   - vypracovanie/aktualizácia bezpečnostnej stratégie,
   - vypracovanie štatútu bezpečnostného výboru,
   - vypracovanie bezpečnostnej politiky.

2) Pre oblasť riadenia rizík:
   - 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,
   - Vykonanie klasifikácie informácií a kategorizácia sietí a informačných systémov,
   - implementáciu systému pre inventarizáciu aktív,
   - vypracovanie interného riadiaceho aktu riadenia rizík kybernetickej a informačnej bezpečnosti,
   - vykonanie riadenie rizík pozostávajúce z identifikácie zraniteľností, identifikácie hrozieb, identifikácie a analýzy rizík podľa metodiky Národného bezpečnostného úradu s ohľadom na aktívum, určenie vlastníka rizika,
   - implementácie organizačných a technických bezpečnostných opatrení,
   - analýzy funkčného dopadu (BIA) a pravidelného preskúmavania identifikovaných rizík v závislosti od aktualizácie prijatých bezpečnostných opatrení.

3) Pre oblasť personálne bezpečnosti:
   - vypracovanie interného riadiaceho aktu s bezpečnostnými zásadami pre koncových používateľov,
   - vypracovanie postupov a procesov upravujúcich personálnu bezpečnosť organizácie prostredníctvom interného riadiaceho aktu,
   - vypracovanie postupov pri zaradení osoby do niektorých z bezpečnostných rolí,
   - vypracovanie postupov pri skončení pracovnoprávneho vzťahu alebo iného obdobného vzťahu,
   - vypracovanie postupov pri porušení bezpečnostných politík.

4) Pre oblasť riadenia prístupov:
   - vypracovanie postupov a procesov upravujúcich riadenie prístupov organizácie a
   - vypracovanie zásad riadenia prístupov osôb k sieti a informačnému systému.

5) Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami
   - vypracovanie interného riadiaceho aktu upravujúceho zásady kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami.

6) Bezpečnosť pri prevádzke informačných systémov a sietí
   - vypracovanie 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.

7) V oblasti hodnotenie zraniteľností a bezpečnostné aktualizácie
   - vypracovanie interného riadiaceho aktu upravujúceho proces riadenia implementácie bezpečnostných aktualizácií a záplat.

8) V oblasti ochrany proti škodlivému kódu

- vypracovanie interného riadiaceho aktu s požiadavkami na určenie zodpovednosti používateľov, pravidiel pre inštaláciu a monitorovania potenciálnych ciest prieniku škodlivého kódu.

9) V oblasti sieťovej a komunikačnej bezpečnosti
   - vypracovanie interného riadiaceho aktu upravujúceho pravidlá sieťovej a komunikačnej bezpečnosti.

10) V oblasti akvizície, vývoja a údržby informačných technológií verejnej správy
   - vypracovanie interného riadiaceho aktu upravujúceho požiadavky na akvizíciu, vývoj a údržbu sietí a informačných systémov, ktoré sa uplatňujú na obstarávané, vyvíjané a udržiavané komponenty s digitálnymi prvkami,
   - vypracovanie metodiky softvérového vývoja v podobe interného riadiaceho aktu, definujúce bezpečnostné požiadavky na všetky fázy životného cyklu vývoja SW (SSDLC) pre vyvíjané produkty – Akademický informačný systém AiS2, portál pre správu projektov CCVaPP.

11) V oblasti zaznamenávanie udalostí a monitorovania
   - vypracovanie dokumentácie spôsobu monitorovania a fungovania Log manažment systému a centrálneho nástroja na bezpečnostné monitorovanie a zadefinovanie spôsobu evidencie prevádzkových záznamov, ich vyhodnocovania, spôsobu hlásenia podozrivej aktivity, zodpovednej osoby a ďalších povinností;
   - vypracovanie interného riadiaceho aktu, ktorý obsahuje a upravuje povinnosti definované platnou legislatívou pre oblasť zaznamenávanie udalostí a monitorovania.

12) V oblasti fyzickej bezpečnosti a bezpečnosti prostredia
   - vypracovanie interného riadiaceho aktu upravujúceho fyzickú bezpečnosť a bezpečnosť prostredia.

13) V oblasti kryptografických opatrení
   - 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 interného riadiaceho aktu upravujúceho systém správy kryptografických kľúčov a certifikátov.

14) V oblasti kontinuity prevádzky
   - vypracovanie interného riadiaceho aktu obsahujúceho a upravujúceho kontinuitu prevádzky následkom kybernetického bezpečnostného incidentu alebo inej krízovej situácie,
   - vykonanie analýzy dopadov na informačné systémy a siete univerzity,
   - vypracovanie stratégie a krízových plánov prevádzky na základe analýzy vplyvov kybernetického bezpečnostného incidentu na informačné systémy a siete univerzity, najmä pre oblasť malvéru, ransomvéru, úniku údajov, rozsiahleho DDoS útoku,
   - vypracovanie postupov zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu alebo inej krízovej situácie.

15) V oblasti auditu a kontrolných činností
   - vypracovanie interného riadiaceho aktu pre oblasti auditu a kontrolných činností v oblasti informačnej a kybernetickej bezpečnosti.

UPJŠ plánuje vyššie uvedené aktivity obstarávať (rozpočtová položka - Vypracovanie dokumentácie a procesov riadenia informačnej a kybernetickej bezpečnosti).

(B) Oblasť riadenie prístupov

V oblasti riadenia prístupov dôjde k revízii aktuálnej bezpečnostnej politiky. UPJŠ si je vedomá toho, že v oblasti riadenia prístupov sú privilegovaní používatelia tou skupinou používateľov, ktorých získanie privilégií má pre organizáciu väčší dopad. V rámci projektu dôjde k zavedeniu prísnejších bezpečnostných opatrení smerom k privilegovaným používateľom z IT oddelení univerzity. To vyžaduje aj zavedenie viacfaktorového overenia vo všetkých systémoch, ktoré to umožňujú.

V rámci projektu budú zakúpené bezpečnostné tokeny na preukázanie identity správcov (rozpočtová položka - Bezpečnostný kľúč).

(C) Oblasť hodnotenia zraniteľností a bezpečnostných aktualizácii

Identifikácia bezpečnostných zraniteľností a následná aplikácia vhodnej formy mitigácie danej zraniteľnosti (napr. vo forme aktualizácie) predstavuje jednu z dôležitých preventívnych opatrení. UPJŠ pravidelne vyhľadáva bezpečnostné zraniteľnosti v rámci svojej infraštruktúry a IT oddelenia jednotlivých pracovísk spoločne s bezpečnostným CSIRT tímom ich následne odstraňujú.

Cieľom tejto podaktivity je rýchla a efektívna identifikácia bezpečnostných zraniteľností a ich odstraňovanie.

V rámci projektu dôjde k revízii bezpečnostnej politiky, identifikácii a hodnotenia zraniteľností a realizácie bezpečnostných aktualizácii, k zakúpeniu licencie nástroja na vyhodnocovanie bezpečnostných zraniteľností (rozpočtová položka - Softvérový nástroj na skenovanie zraniteľností) a k realizácii minimálne dvoch vyhodnocovaní bezpečnostných zraniteľností.

(D) Oblasť zaznamenávania udalostí a monitorovanie

Zaznamenávanie udalostí z infraštruktúry organizácie je nevyhnutné k tomu, aby bolo možné následne identifikovať vzniknuté bezpečnostné incidenty. UPJŠ disponuje vlastným CSIRT tímom, ktorého úlohou je aj monitorovanie infraštruktúry a správa bezpečnostných technológií pre takýto monitoring. Tento bezpečnostný tím pracuje s bezpečnostnými technológiami od spoločností Microsoft a ESET a využíva aktuálne dostupné možnosti týchto technológií. To sa v súčasnej dobe ukazuje ako nedostačujúce a je nevyhnutné implementovať plnohodnotný SIEM systém.

V rámci tejto aktivity je plánované obstaranie hardvérových a softvérových častí pre dohľadovú časť bezpečnostného tímu. To si bude vyžadovať implementáciu centrálneho manažmentu logov a SIEM systému v prostredí UPJŠ. Bude zavedené pre kritické sieťové prvky UPJŠ, centrálny sieťový prvok a kritické informačné systémy a služby univerzity. Predpokladá sa zapojenie 120 týchto systémov, sieťových prvkov, centrálneho firewallu vrátane infraštruktúry nevyhnutnej pre vývoj akademického informačného systému AiS2.

Cieľom tejto podaktivity je rýchla a efektívna identifikácia bezpečnostných udalostí a kybernetických bezpečnostných incidentov.

V rámci projektu sa bude obstarávať SIEM systém, ktorého súčasťou je aj log manažment (softvér, hardvér, implementácia, nastavenie pravidiel) (rozpočtová položka - LMS a SIEM). Súčasne dôjde k zakúpeniu technickej časti dohľadového centra – 2 väčších obrazoviek a 4 pracovných staníc, dedikovaných pre prácu s bezpečnostnými technológiami implementovanými na UPJŠ (rozpočtová položka - IT pre dohľadové centrum). Navyše je nutné bezpečne uchovávať záznamy a výsledne analýzy. K tomuto účelu bude zakúpené ďalší úložný priestor (rozpočtová položka - Dátové úložisko NAS).

Položky (LMS a SIEM, IT pre dohľadové centrum, Dátové úložisko NAS) ktoré bude UPJŠ obstarávať v rámci projektu, budú tvoriť funkčný celok dohľadového centra, oddelený od ostatnej prevádzkovej infraštruktúry.

(E) Oblasť riešenia kybernetických bezpečnostných incidentov

Ako už bolo vyššie spomenuté UPJŠ disponuje vlastným bezpečnostným tímom (CSIRT-UPJS) a súčasne aj procesným riadením riešenia kybernetických bezpečnostných incidentov.

V rámci projektu je cieľom zvýšiť adekvátnosť reakcie na kybernetické bezpečnostné incidenty, ale aj schopnosti predchádzať týmto bezpečnostným incidentom. V rámci projektu dôjde k zakúpeniu internej infraštruktúry bezpečnostného tímu, ktorá slúži na prevádzku systémov pre vyhľadávanie bezpečnostných zraniteľností, evidenciu bezpečnostných incidentov, vyhľadávanie verejne dostupných zdrojov a informácii o bezpečnostných hrozbách a pod. (rozpočtové položky – Server, Záložný zdroj 2, Switch).

(I) Sieťová a komunikačná bezpečnosť

Počítačová sieť a iné komunikačné siete v súčasnej dobe predstavujú neoddeliteľnú súčasť poskytovania rôznych služieb. V rámci projektu plánujeme obstarať Firewall novej generácie (rozpočtové položky – Firewall a Záložný zdroj 1), ktoré umožnia UPJŠ lepšie zabezpečenie perimetra lokálnej počítačovej siete SAUNET a efektívnejšie riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami. Navyše nový typ Firewallu bude umožňovať efektívnejší manažment pravidiel, identifikáciu neoprávnených sieťových spojení na hranici s vonkajšou sieťou, blokovanie neoprávnených spojení, monitorovanie bezpečnosti, detekciu prienikov a prevenciu prienikov (IPS a IDS) identifikáciou nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky.

Cieľom tejto podaktivity je súčasne aj zefektívnenie identifikácie bezpečnostných udalostí tým, že sa budú zasielať sieťové záznamy a netflow z centrálneho sieťového zariadenia do LMS/ SIEM.

(P) Audit a kontrolné činnosti

V rámci dokončovacej fázy projektu budú realizované dve aktivity, ktorých účelom je overenie kvality implementovaných procesov a bezpečnostných opatrení. Dôjde k realizácii auditu kybernetickej bezpečnosti v zmysle zákona o kybernetickej bezpečnosti a vykonávacieho právneho predpisu. Tento externý audit považujeme za vhodné zhodnotenie stavu informačnej a kybernetickej bezpečnosti na konci realizovaného projektu. Navyše dôjde k realizácii bezpečnostného auditu webovej aplikácie akademického informačného systému AiS2.

Dôležitým a špecifickým aspektom projektu je zvýšenie bezpečnosti vývoja Akademického informačného systému AiS2. Ako sme už vyššie uviedli, tento informačný systém sa využíva na 17 univerzít vyše 75.000 používateľmi. Výskyt bezpečnostného incidentu, resp. objavenie bezpečnostnej zraniteľnosti môže mať negatívny vplyv na informačnú a kybernetickú bezpečnosť ďalších 16 inštitúcii. Z tohto dôvodu všetky plánované činnosti (podaktivity) sa zameriavajú aj na tento vývoj. Implementácia LMS a SIEM zahrnie aj vývojovú infraštruktúru AIS2. V projekte bude vypracovaná a aplikovaná metodika softvérového vývoja v podobe interného riadiaceho aktu, definujúce bezpečnostné požiadavky na všetky fázy životného cyklu vývoja SW (SSDLC) pre tento informačný systém.

4. ARCHITEKTÚRA RIEŠENIA PROJEKTU

4.1 Biznis vrstva

Predmetom projektu je riadenie informačnej a kybernetickej bezpečnosti a realizácia bezpečnostných opatrení definovaných v právnej úprave, najmä v zákone č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon o KB“) a zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ITVS“).

Predmetom projektu sú najmä tie oblasti, kde žiadateľ identifikoval najvyššiu mieru rizika a najvyššie dopady. Pri výbere a nastavení oprávnených podaktivit žiadateľ vychádzal najmä z požiadaviek určených právnou úpravou. Jednotlivé biznis funkcie (podaktivity výzvy realizovane v rámci projektu) bezpečnostnej architektúry sú znázornene na Obr. 1.

Obr. 1 Business architektúra

4.1.1 Prehľad koncových služieb – budúci stav

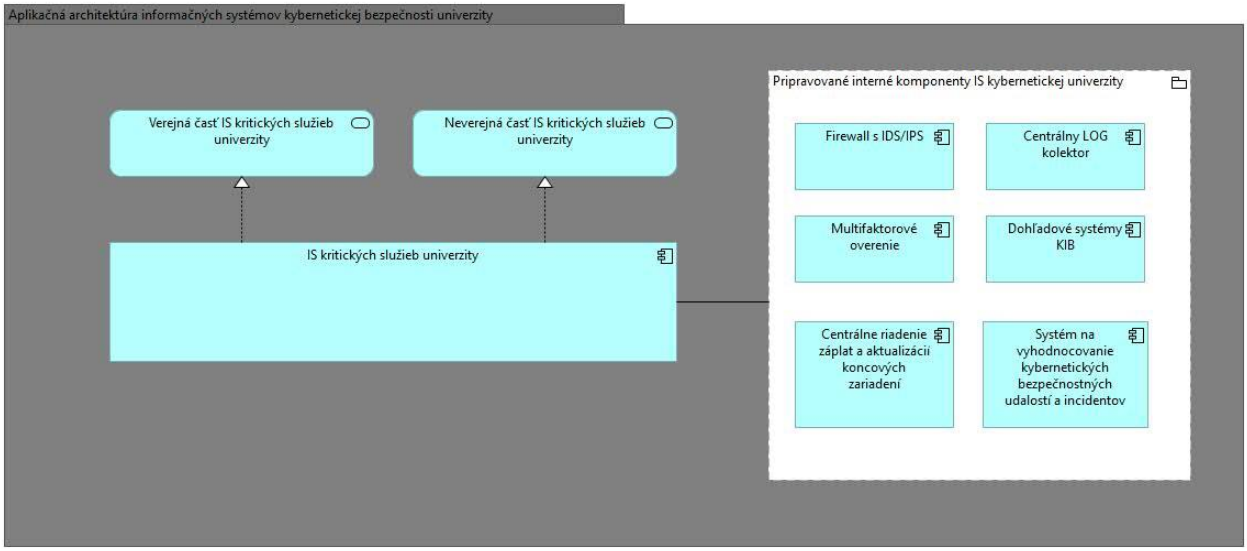
Predmetom projektu nie je budovanie koncových služieb.

4.1.2 Jazyková podpora a lokalizácia

Predmetom projektu nie je dodávka informačného systému. Výstupy (produkty) budú dodávané v slovenskom jazyku.

4.2 Aplikačná vrstva

Aplikačnú architektúru projektu tvoria riešenia pre oblasť informačnej a kybernetickej bezpečnosti zobrazené na Obr. 2. K pripravovaným interným komponentom IS patrí **firewall s IDS/IPS** na kontrolu sieťovej prevádzky s funkciou detekcie a prevencie narušenia, **Centrálny LOG kolektor** na zber a centralizáciu logovacích údajov, zavedenie **multifaktorového overenia,** implementácia **dohľadových systémov** a **systému na vyhodnocovanie kybernetických bezpečnostných udalostí,** ktoré identifikujú potenciálne bezpečnostné hrozby. Súčasťou bude aj **centrálne riadenie záplat a aktualizácií,** čo umožní rýchlo reagovať na nové zraniteľnosti koncových zariadení.



Obr. 2 Aplikačná architektúra projektu

4.2.1 Rozsah informačných systémov – AS IS

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)*
14274	Akademický informačný systém Ais2	☐	Prevádzkovaný a plánujem rozvíjať	Agendový	
14275	Microsoft 365 - UPJŠ	☐	Prevádzkovaný a plánujem rozvíjať	Agendový	
14276	Knižničný informačný systém Aleph	☐	Prevádzkovaný a plánujem rozvíjať	Agendový	
14277	E-learning Moodle	☐	Prevádzkovaný a plánujem rozvíjať	Agendový	
14278	Portál CCVaPP	☐	Prevádzkovaný a plánujem rozvíjať	Agendový	
14279	CMS webového sídla univerzity	☐	Prevádzkovaný a plánujem rozvíjať	Prezentačný	
14280	Správa siete UPJŠ	☐	Prevádzkovaný a plánujem rozvíjať	Agendový	
14281	Registratúrny systém	☐	Prevádzkovaný a plánujem rozvíjať	Ekonomický a administratívny chod inštitúcie	

4.2.2 Rozsah informačných systémov – TO BE

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)*
14274	Akademický informačný systém AiS2	☐	Prevádzkovaný a plánujem rozvíjať	Agendový	
14275	Microsoft 365 - UPJŠ	☐	Prevádzkovaný a plánujem rozvíjať	Agendový	
14276	Knižničný informačný systém Aleph	☐	Prevádzkovaný a plánujem rozvíjať	Agendový	
14277	E-learning Moodle	☐	Prevádzkovaný a plánujem rozvíjať	Agendový	
14278	Portál CCVaPP	☐	Prevádzkovaný a plánujem rozvíjať	Agendový	
14279	CMS webového sídla univerzity	☐	Prevádzkovaný a plánujem rozvíjať	Prezentačný	
14280	Správa siete UPJŠ	☐	Prevádzkovaný a plánujem rozvíjať	Agendový	
14281	Registratúrny systém	☐	Prevádzkovaný a plánujem rozvíjať	Ekonomický a administratívny chod inštitúcie	

4.2.3 Využívanie nadrezortných a spoločných ISVS – AS IS

Predmetom projektu nie je využívanie nadrezortných alebo spoločných ISVS.

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

Predmetom projektu nie je realizácia integrácií ISVS na nadrezortné ISVS.

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

Predmetom projektu nie je využívania iných ISVS.

4.2.6 Aplikačné služby pre realizáciu koncových služieb – TO BE

Predmetom projektu nie sú aplikačné služby pre realizáciu koncových služieb.

4.2.7 Aplikačné služby na integráciu – TO BE

Predmetom projektu nie je realizácia integrácii.

4.2.8 Poskytovanie údajov z ISVS do IS CSRÚ – TO BE

Predmetom projektu nie je poskytovanie údajov do IS CSRU.

4.2.9 Konzumovanie údajov z IS CSRÚ – TO BE

Predmetom projektu nie je konzumovanie údajov z IS CSRÚ.

4.3 Dátová vrstva

4.3.1 Údaje v správe organizácie

Predmetom projektu nie je spracovanie údajov ako objektmi evidencie.

4.3.2 Dátový rozsah projektu - Prehľad objektov evidencie - TO BE

Predmetom projektu nie je spracovanie údajov ako objektmi evidencie.

4.3.3 Referenčné údaje

Projekt nepracuje s referenčnými údajmi.

4.3.4 Kvalita a čistenie údajov

Predmetom projektu nie je kvalita a čistenie údajov.

4.3.5 Otvorené údaje

Predmetom projektu nie je riešenie otvorených údajov.

4.3.6 Analytické údaje

Predmetom projektu nie je riešenie analytických údajov.

4.3.7 Moje údaje

Predmetom projektu nie je riešenie „Moje údaje“.

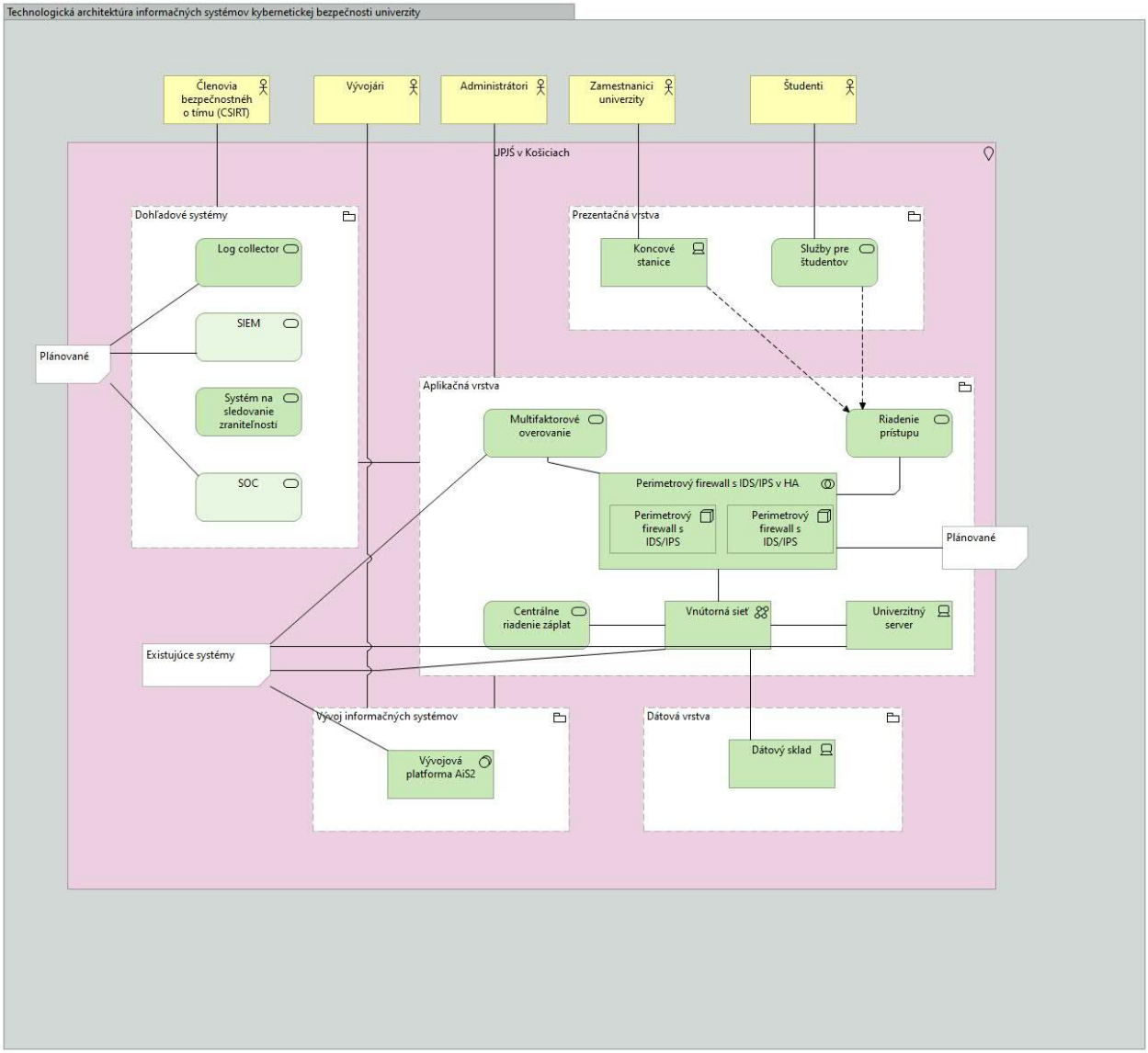
4.3.8 Prehľad jednotlivých kategórií údajov

Predmetom projektu nie sú prehľady kategórií údajov.

4.4 Technologická vrstva

S ohľadom na inštrukcie Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky neuvádzame podrobný prehľad aktuálneho technologického stavu (AS IS). Konštatujeme však, že pre zaistenie kybernetickej a informačnej bezpečnosti je potrebné aktuálny stav doplniť tak, aby bezpečnostné opatrenia boli v súlade s požiadavkami zákona o kybernetickej bezpečnosti a súvisiacej právnej úpravy.

Technologickú vrstvu popisuje Obr. 3, na ktorom sú označené aktuálne a plánované prvky. K plánovaným prvkom patrí perimetrový firewall (2ks) v „high availability“ móde so systémom detekcie a prevencie prienikov (IPS/IDS, infraštruktúra pre SOC, SIEM a log kolektor (s uchovaním dát po dobu 18 mesiacov).



Obr. 3 Technologická architektúra projektu

4.4.1 Požiadavky na výkonnostné parametre, kapacitné požiadavky – TO BE

Parameter	Jednotky	Predpokladaná hodnota	Poznámka
Počet interných používateľov	Počet	9500	Počet zamestnancov a študentov UPJŠ
Počet maximálneho počtu udalostí spracovaných za 1 sekundu	EPS	20000	
Maximálny objem dát cez centrálny firewall	Gps	10	

4.4.2 Návrh riešenia technologickej architektúry

Predmetom projektu nie je využívanie služieb vládneho cloudu, vývoj nových ITVS.

4.4.3 Využívanie služieb z katalógu služieb vládneho cloudu

Predmetom projektu nie je využívanie služieb vládneho cloudu.

4.5 Bezpečnostná architektúra

V súčasnosti sú na UPJŠ implementované bezpečnostné opatrenia vyžadované platnou právnou úpravou len čiastočne. požadované platnou legislatívou, ako vyplýva z projektového zámeru. Navrhovaná architektúra riešenia na dosiahnutie TO BE stavu bude znamenať zvýšenie súladu s nasoľujúcimi právnymi predpismi:

- *Zákon č. 95/2019 Z.z. o informačných technológiách vo verejnej správe*
- *Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti*
- *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

Predmetom projektu nie je vývoj a dodanie informačného systému. Z tohto dôvodu táto časť nie je relevantná pre projekt.

7. PREVÁDZKA A ÚDRŽBA

7.1 Prevádzkové požiadavky

7.1.1 Úrovne podpory používateľov

Help Desk bude realizovaný cez 2 úrovne podpory, s nasledujúcim označením:

- ***L1 podpory IS** (Level 1, priamy kontakt zákazníka) - jednotný kontaktný bod verejného obstarávateľa – IS Solution manager, ktorý je v správe verejného obstarávateľa a v prípade jeho nedostupnosti Centrum podpory používateľov (zabezpečuje prevádzkovateľ IS a DataCentrum).*
- ***L2 podpory IS** (Level 2, postúpenie požiadaviek od L1) - vybraná skupina garantov, so znalosťou IS (zabezpečuje prevádzkovateľ IS – verejný obstarávateľ).*

Definícia:

- ***Podpora L1 (podpora 1. stupňa)** - začiatočná úroveň podpory, ktorá je zodpovedná za riešenie základných problémov a požiadaviek koncových užívateľov a ďalšie služby vyžadujúce základnú úroveň technickej podpory. Základnou funkciou podpory 1. stupňa je zhromaždiť informácie, previesť základnú analýzu a určiť príčinu problému a jeho klasifikáciu. Typicky sú v úrovni L1 riešené priamočiare a jednoduché problémy a základné diagnostiky, overenie dostupnosti jednotlivých vrstiev infraštruktúry (sieťové, operačné, vizualizačné, aplikačné atď.) a základné užívateľské problémy (typicky zabudnutie hesla), overovanie nastavení SW a HW atď.*
- ***Podpora L2 (podpora 2. stupňa)** – riešiteľské tímy s hlbšou technologickou znalosťou danej oblasti. Riešitelia na úrovni Podpory L2 nekomunikujú priamo s koncovým užívateľom, ale sú zodpovední za poskytovanie súčinnosti riešiteľom 1. úrovne podpory pri riešení eskalovaného hlásenia, čo mimo iného obsahuje aj spätnú kontrolu a podrobnejšiu analýzu zistených dát predaných riešiteľom 1. úrovne podpory. Výstupom takejto kontroly môže byť potvrdenie, upresnenie, alebo prehodnotenie hlásenia v závislosti na potrebách Objednávateľa. Primárnym cieľom riešiteľov na úrovni Podpory L2 je dostať hlásenie čo najskôr pod kontrolu a následne ho vyriešiť.*

Pre služby sú definované takéto SLA:

- *Help Desk je dostupný cez platformu LiveAgent, incidenty sú evidované v platforme LiveAgent.*
- *Dostupnosť L2 podpory pre IS je 8x5 (8 hodín x 5 dní od 8:00h do 16:00h počas pracovných dní).*

7.1.2 Riešenie incidentov – SLA parametre

Požadované SLA na služby systémovej a aplikačnej podpory – servisné služby vzťahujúce sa na produkčné a testovacie prostredie IS Úrovne podpory používateľov: Help Desk bude realizovaný cez 2 úrovne podpory, s nasledujúcim označením:

- L1 podpory IS (Level 1, priamy kontakt zákazníka) - jednotný kontaktný bod verejného obstarávateľa.
- L2 podpory IS (Level 2, postúpenie požiadaviek od L1) - vybraná skupina garantov, so znalosťou IS (zabezpečuje prevádzkovateľ IS – verejný obstarávateľ).

Definície:

Podpora L1 (podpora 1. stupňa) - začiatočná úroveň podpory, ktorá je zodpovedná za riešenie základných problémov a požiadaviek koncových užívateľov a ďalšie služby vyžadujúce základnú úroveň technickej podpory. Základnou funkciou podpory 1. stupňa je zhromaždiť informácie, previesť základnú analýzu a určiť príčinu problému a jeho klasifikáciu. Typicky sú v úrovni L1 riešené priamočiare a jednoduché problémy a základné diagnostiky, a základné užívateľské problémy (typicky zabudnutie hesla), overovanie nastavení SW a HW atď.

Podpora L2 (podpora 2. stupňa) – riešiteľské tímy s hlbšou technologickou znalosťou v danej oblasti. Riešitelia na úrovni Podpory L2 sú zodpovední za poskytovanie súčinnosti riešiteľom 1. úrovne podpory pri riešení eskalovaného hlásenia, čo mimo iného obsahuje aj spätnú kontrolu a podrobnejšiu analýzu zistených dát odovzdaných riešiteľmi 1. úrovne podpory. Výstupom takejto kontroly môže byť potvrdenie, upresnenie, alebo prehodnotenie hlásenia v závislosti na potrebách. Primárnym cieľom riešiteľov na úrovni Podpory L2 je riešenie najobtiažnejších hlásení, vrátane vykonávania hĺbkových analýz a riešenie extrémnych prípadov.

Riešenie incidentov – SLA parametre Za incident je považovaná chyba IS, t.j. správanie sa v rozpore s prevádzkovou a používateľskou dokumentáciou IS. Za incident nie je považovaná chyba, ktorá nastala mimo prostredia IS napr. výpadok poskytovania konkrétnej služby.

Označenie naliehavosti incidentu:

Označenie naliehavosti incidentu	**Závažnosť incidentu**	**Popis naliehavosti incidentu**
A	Kritická	Kritické chyby, ktoré spôsobia úplné zlyhanie systému ako celku a nie je možné používať ani jednu jeho časť, nie je možné poskytnúť požadovaný výstup z IS.
B	Vysoká	Chyby a nedostatky, ktoré zapríčinia čiastočné zlyhanie systému a neumožňuje používať časť systému.
C	Stredná	Chyby a nedostatky, ktoré spôsobia čiastočné obmedzenia používania systému.
D	Nízka	Kozmetické a drobné chyby.

možný dopad:

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

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

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

Vyžadované reakčné doby:

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

7.2 Požadovaná dostupnosť IS:

Popis	Parameter	Poznámka
Prevádzkové hodiny	*12 hodín*	*od 6:00 hod. - do 18:00 hod. počas pracovných dní*
Servisné okno	*10 hodín*	*od 19:00 hod. - do 5:00 hod. počas pracovných dní*
	24 hodín	*od 00:00 hod. - 23:59 hod. počas dní pracovného pokoja a štátnych sviatkov* *Servis a údržba sa bude realizovať mimo pracovného času.*
Dostupnosť produkčného prostredia IS	*95%*	*95% z 24/7/365 t.j. max ročný výpadok je 438 hod.* *Maximálny mesačný výpadok je 36,5 hodiny.* *Vždy sa za takúto dobu považuje čas od 0.00 hod. do 23.59 hod. počas pracovných dní v týždni.* *Nedostupnosť IS sa počíta od nahlásenia incidentu Zákazníkom v čase dostupnosti podpory Poskytovateľa (t.j. nahlásenie incidentu na L2 v čase od 6:00 hod. - do 18:00 hod. počas pracovných dní). Do dostupnosti IS nie sú započítavané servisné okná a plánované odstávky IS.* *V prípade nedodržania dostupnosti IS bude každý ďalší začatý pracovný deň nedostupnosti braný ako deň omeškania bez odstránenia vady alebo incidentu.*

7.2.1 Dostupnosť (Availability)

***Dostupnosť** (**Availability**) je pojem z oblasti riadenia bezpečnosti v organizácii. Dostupnosť znamená, že dáta sú prístupné v okamihu jej potreby. Narušenie dostupnosti sa označuje ako nežiaduce zničenie (destruction) alebo nedostupnosť. Dostupnosť je zvyčajne vyjadrená ako percento času v danom období, obvykle za rok. Orientačný zoznam dostupnosti je uvedený v nasledovnom prehľade:*

- ***95% dostupnosť** znamená výpadok 18,25 dňa*

7.2.2 RTO (Recovery Time Objective)

Recovery Time Objective *(zvyčajne sa požíva skratka RTO) je jeden z ukazovateľov dostupnosti dát. RTO vyjadruje množstvo času potrebné pre obnovenie dát a celej prevádzky nedostupného systému (softvér). Môže byť, v závislosti na použitej technológii, vyjadrené v sekundách, hodinách či dňoch.*

- *Tradičné zálohovanie - výpadok a obnova trvá cca hodiny až dni podľa dotknutého IS.*

7.2.3 RPO (Recovery Point Objective)

Recovery Point Objective *(zvyčajne sa požíva skratka RPO) je jeden z ukazovateľov dostupnosti dát. RPO vyjadruje, do akého stavu (bodu) v minulosti možno obnoviť dáta. Inými slovami množstvo dát, o ktoré môže organizácia prísť.*

- *Tradičné zálohovanie - výpadok a obnova trvá cca hodiny až dni podľa dotknutého IS.*

8. POŽIADAVKY NA PERSONÁL

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

- Predseda RV – prof. MUDr. Pavol Jarčuška, PhD.
- Biznis vlastník - doc. RNDr. JUDr. Pavol Sokol, PhD.
- Zástupca prevádzky – Ing. Jozef Jantošovič
- Projektový manažér objednávateľa (PM) – Ing. Katarína Pezlarová

Pre účely realizácie projektu sa zostavuje **Projektový tím objednávateľa** v nasledovnom zložení:

- manažér IT prevádzky - Ing. Miroslav Pomikala
- manažér IT prevádzky – RNDr. Radovan Engel, PhD.
- IT analytik – Bc. Michal Šafranko
- Architekt IT – Mgr. Slavomír Varchula
- kľúčový používateľ – Bc. Jakub Mohler
- kľúčový používateľ – Bc. Monika Rapavá
- kľúčový používateľ – Bc. Zuzana Hennelová
- kľúčový používateľ – Ing. Ján Ondrej
- kľúčový používateľ – Mgr. Miroslav Baranko
- kľúčový používateľ – Ing. Patrícia Kočiščáková
- kľúčový používateľ – Mgr. Katarína Varchulová

ID	Meno a Priezvisko	Pozícia	Oddelenie	Rola v projekte
1.	prof. MUDr. Pavol Jarčuška, PhD.	Prorektor UPJŠ	Rektorát UPJŠ	Predseda riadiaceho výboru
2.	Ing. Jozef Jantošovič	Riaditeľ CIaKT	CIaKT UPJŠ	Zástupca prevádzky
3.	doc. RNDr. JUDr. Pavol Sokol, PhD.	Vedúci úseku informačnej a kybernetickej bezpečnosti CIaKT	CIaKT UPJŠ - CSIRT-UPJS	Manažér kybernetickej a informačnej bezpečnosti / Biznis vlastník
4.	Ing. Katarína Pezlarová	Projektový manažér	CCVaPP UPJŠ	Projektový manažér
5.	Ing. Miroslav Pomikala	Vedúci úseku Správca operačných systémov	CIaKT UPJŠ	manažér IT prevádzky
6.	RNDr. Radovan Engel, PhD.	Vedúci vývojového tímu AiS2	CIaKT UPJŠ – vývoj AiS2	manažér IT prevádzky
7.	Bc. Michal Šafranko	Člen bezpečnostného tímu, bezpečnostný analytik	CIaKT UPJŠ - CSIRT-UPJS	IT analytik
8.	Mgr. Slavomír Varchula	Člen vývojového tímu AiS2, architekt	CIaKT UPJŠ – vývoj AiS2	Architekt IT
9.	RNDr. Patrik Pekarčík	Člen bezpečnostného tímu, administrátor internej infraštruktúry	CIaKT UPJŠ - CSIRT-UPJS	kľúčový používateľ
10.	Bc. Jakub Mohler	Člen bezpečnostného tímu, incident handler	CIaKT UPJŠ - CSIRT-UPJS	kľúčový používateľ
11.	Bc. Monika Rapavá	Členka bezpečnostného tímu, incident handler	CIaKT UPJŠ - CSIRT-UPJS	kľúčový používateľ
12.	Bc. Zuzana Hennelová	Členka bezpečnostného tímu, incident handler	CIaKT UPJŠ - CSIRT-UPJS	kľúčový používateľ
13.	Ing. Ján Ondrej	Administrátor centrálnej infraštruktúry	CIaKT UPJŠ	kľúčový používateľ
14.	Mgr. Miroslav Baranko	Administrátor centrálnej infraštruktúry	CIaKT UPJŠ	kľúčový používateľ
15.	Ing. Patrícia Kočiščáková	Administrátor vývojovej infraštruktúry AiS2	CIaKT UPJŠ – vývoj AiS2	kľúčový používateľ
16.	Mgr. Katarína Varchulová	Špecialista zákazníckej podpory	CIaKT UPJŠ – vývoj AiS2	kľúčový používateľ

Pracovné náplne pre vyššie uvedené projektové role:

Predseda riadiaceho výboru - zodpovedá za celkové riadenie a dohľad nad projektom.

1. Koordinuje činnosť riadiaceho výboru, vedie zasadnutia a zodpovedá za schvaľovanie hlavných rozhodnutí projektu.
2. Zabezpečuje, aby projekt napĺňal svoje ciele a bol v súlade s dohodnutým harmonogramom a rozpočtom.
3. Zabezpečuje komunikáciu s vedením univerzity, predkladá správy o projekte vedeniu, predkladá podklady na schválenie vedeniu univerzity.

Zástupca prevádzky - je zodpovedný za prevádzkové aspekty projektu.

1. Zabezpečuje, aby implementácia a prevádzka riešení prebiehala hladko a efektívne.
2. Poskytuje podporu a informácie potrebné pre úspešné dokončenie projektu a riešenie prevádzkových problémov.
3. Rieši rozpory medzi prevádzkou IT infraštruktúry a zabezpečením IT.
4. Pripravuje technické podklady pre riadenie projektu.
5. V prípade neprítomnosti predsedu riadiaceho výboru ho zastupuje na jednaniach.

Manažér kybernetickej a informačnej bezpečnosti - zodpovedá za dodržanie princípov a štandardov kybernetickej a informačnej bezpečnosti.

1. Koordinuje a riadi činnosť v oblasti kybernetickej a informačnej bezpečnosti.
2. Navrhuje implementácie bezpečnostných opatrení a kontroluje ich dodržiavanie.
3. Realizuje testy bezpečnostných opatrení a kybernetickej bezpečnosti.
4. Poskytuje poradenstvo v oblasti kybernetickej a informačnej bezpečnosti.
5. Zabezpečuje súlad s legislatívnymi požiadavkami.
6. Špecifikuje a analyzuje funkčné požiadavky na kybernetickú a informačnú bezpečnosť.
7. **Pripravuje technické podklady pre riadenie projektu.**

Biznis vlastník - zodpovedá za procesy a výstupy projektu, ktoré sú určené pre konečných používateľov. Zodpovedá za prínos projektových riešení pre konečných používateľov.

1. Schvaľuje biznis požiadavky a zabezpečuje, aby projektové riešenia prinášali požadovanú hodnotu a prínosy..
2. Definuje očakávania na kvalitu projektu a schvaľuje akceptačné kritériá..
3. Definuje schvaľovanie akceptačných kritérií.

Projektový manažér - zodpovedá za riadenie projektu počas jeho celého životného cyklu.

1. Riadi projektové zdroje.
2. Zabezpečuje tvorbu obsahu a neustále odôvodňovanie projektu.
3. Koordinuje činnosti členov projektového tímu.
4. Sleduje dodržiavanie harmonogramu a rozpočtu.
5. Rieši riziká súvisiace s implementáciou projektu.

Manažér IT prevádzky - zodpovedá za riadenie, prevádzku, alebo vývoj informačných a komunikačných technológií a informačných systémov (v rozsahu zodpovednosti v rámci organizačnej štruktúry organizácie tak, aby spĺňal požiadavky a potreby projektu).

1. Zabezpečuje plynulý chod informačných a komunikačných technológií.
2. Spravuje hardvérové a softvérové vybavenie.
3. Rieši technické problémy v rámci projektu..
4. Koordinuje činnosť tímu administrátorov.
5. Zaisťuje bezpečnosť a efektívnosť IT prevádzky.

IT analytik - zodpovedá za zber a analýzu funkčných požiadaviek, tvorbu špecifikácií a návrh riešení v rámci projektu.

1. Spolupracuje na vývoji nových aplikácií a vylepšovaní existujúcich systémov.
2. Vykonáva zber a analýzu funkčných požiadaviek.
3. Tvorí špecifikácie a návrhy riešení.
4. Analyzuje potreby zákazníka a poskytuje vstupy pre architektov a vývojárov riešení.
5. Spolupracuje na vývoji nových aplikácií a vylepšovaní existujúcich systémov.
6. Poskytuje vstupy pre ostatných členov projektového tímu.

Architekt IT - zodpovedá za návrh architektúry IT riešení a implementáciu technológií systémov (v rozsahu zodpovednosti v rámci organizačnej štruktúry organizácie tak, aby spĺňal požiadavky a potreby projektu).

1. Navrhuje systémy tak, aby dosahovali najlepšiu efektivitu a flexibilitu.
2. Implementácia technológií.
3. Zabezpečuje technickú dokumentáciu
4. Kontroluje súlad implementácie s návrhom.
5. Posudzuje vhodnosť navrhnutých riešení.

Kľúčový používateľ - zodpovedá za prevádzku projektových produktov, ich plnohodnotné využitie v zmysle projektu.

1. Navrhuje a špecifikuje funkčné a technické požiadavky.
2. Vykonáva akceptačné testovanie
3. Zabezpečuje, aby riešenia spĺňali potreby koncových používateľov.
4. Definuje požiadavky a potreby koncových používateľov.

9. IMPLEMENTÁCIA A PREBERANIE VÝSTUPOV PROJEKTU

Projekt bude v zmysle Vyhlášky MIRRI o riadení projektov realizovaný metódou Waterfall s logickými nadväznosťami realizácie jednotlivých modulov na základe funkčnej a technickej špecifikácie vypracovanej v rámci prípravy projektu. Súčasne predmetný projekt bude vzhľadom na previazanosť jednotlivých aktivít realizovaný v rámci jedného samostatného inkrementu.

10. PRÍLOHY

Dokument neobsahuje prílohy.