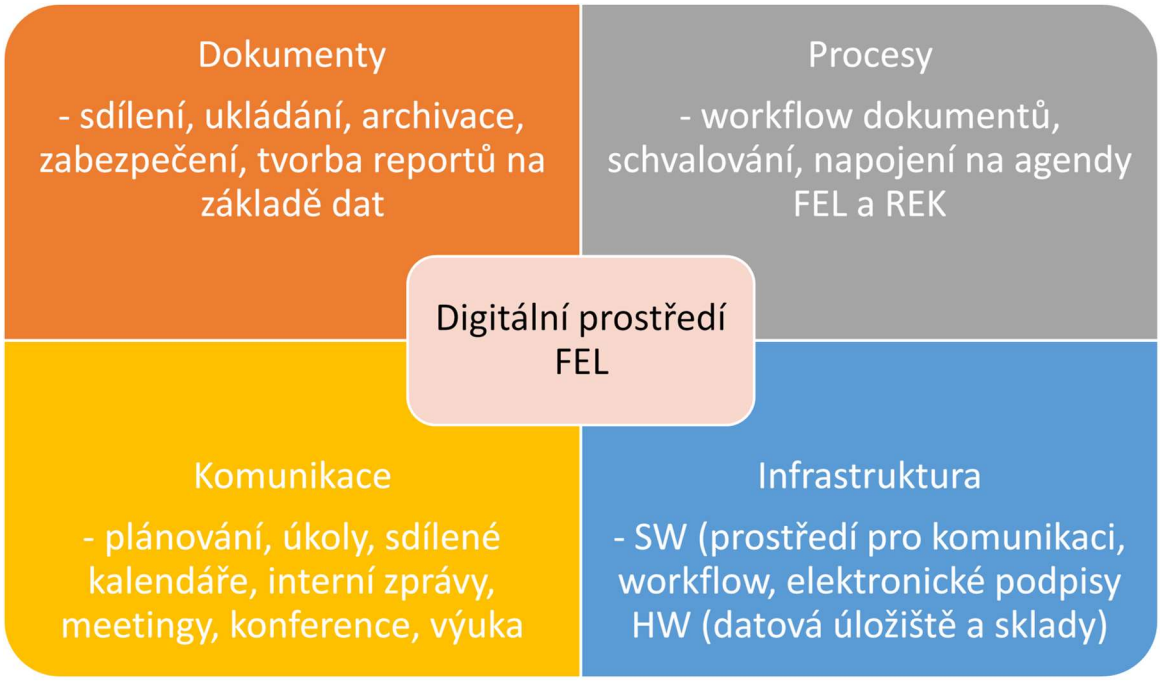
Technické a funkční specifikace na IS FEL

Obsah

1 Shrnutí

1.1 Hlavní cíle

Zadavatel má za cíl pořídit informační systém (IS), který umožní realizaci elektronizaci agend a vytvořit digitální prostředí FEL ZČU. Hlavní oblasti řešení jsou uvedeny na obrázku 1.



Elektronizace agend fakulty a vytvořené digitální prostředí má za cíl snížení administrativní náročnosti provozních procesů FEL, dále snížení nákladů na tyto činnosti, úsporu času a zajištění vhodné podpory. Nový IS musí splnit požadavky na konektivitu se stávajícími IS ZČU, které jsou v rámci ZČU používány.

Dále zadavatel klade důraz na splnění bezpečnostních požadavků a zásad ochrany osobních údajů. Provozní bezpečnost bude zajištěna systémem opatření vycházejících z ISO 27002:2023 a sadou technických nástrojů pro sledování a vyhodnocování provozu, správy logů, propracovaným systémem managementu kontinuity podnikání a dalšími nástroji a opatřeními.

Jednotlivé komponenty dodávaného systému mají být provozovány v cloudu a to vždy ve shodě s platnými bezpečnostními předpisy. Poskytovatel cloudových služeb musí garantovat, že data budou vždy uložena na serverech v rámci EU. Technologické prostředky k nasazení je nezbytné konzultovat s CIV (Centrum Informatizace a Výpočetní Techniky), která zajišťuje a koordinuje informační technologie v rámci ZČU.

V současné době jsou používána jak on-premise tak cloudová řešení od MS a Google. Většina zaměstnanců využívá nástroje a platformy Microsoft 365. Fakulta využívá konkrétně licence Microsoft 365 Education A3 . V rámci univerzitního prostředí má zadavatel zajištěnou jednotnou bezpečnost včetně konektivity k aktuálně používaným cloudovým službám. Dokumenty v rámci spisové služby ZČU jsou uloženy na vlastním serveru ZČU. ZČU využívá spisovou službu eSpis od dodavatele ICZ.

1.2 Koncept řešení

K dosažení úspěšné realizace požaduje zadavatel dodávku a implementaci informačního systému a MIS (Manažerského informačního systému) s následnou integrací na požadované informační systémy zadavatele. Rozsah potřebné integrace bude specifikován v Předimplementační analýze. Zadavatel připouští možnost, že pro jádro navrhovaného řešení může být použita platforma Microsoft Office 365.

Zadavatel předpokládá realizaci projektu v těchto milnících:

1. Vypracování Iniciační dokumentace a Předimplementační analýzy (PIA) v časovém rozmezí 3-4 měsíců.

2. Provedení Implementace v časovém rozmezí 6-9 měsíců.

3. Testovací provoz v rozsahu minimálně 1 měsíc.

4. Ostrý provoz.

5. Poskytnutí garantované servisní podpory po dobu minimálně 3 let.

V rámci Předimplementační analýzy požaduje zadavatel zpracování analýzy standardních procesů, nejlepší praxe implementovaného řešení a specifických potřeb jednotlivých pracovišť FEL. Cílem analýzy bude aktualizace procesního modelu FEL a souvisejících procesů pro potřeby implementace vlastního řešení. Předimplementační analýza bude také zahrnovat upřesnění požadavků k řešení platných k období, kdy bude analýza prováděna. FEL se zavazuje poskytnout dodavateli potřebnou součinnost zaměstnanců.

Licence operačního systému a databází mohou být součástí dodávky, je však nutno zohlednit akademickou povahu zadavatele a pro něj dostupné licenční modely. Dodavatel v rámci Předimplementační analýzy vyspecifikuje požadavky na technologickou infrastrukturu tak, aby aplikační software zohledňoval minimální požadavky na technickou dostupnost systému, požadavky na výkonnostní škálovatelnost systému, zálohování a případnou obnovu systému. Serverová část systému musí mít možnost navýšení výkonu při nárůstu počtu uživatelů.

Dále zadavatel požaduje servisní podporu, která bude financována již výhradně z jeho vlastních prostředků. Součástí servisní podpory je kromě podpory a údržby aplikace dodávaného řešení i jeho systémová podpora. Zadavatel předpokládá vyškolení vlastních zaměstnanců pro správu jednotlivých částí systému. Dále zadavatel také předpokládá, že úspěšná implementace v rámci FEL ZČU může být rozšířena i na ostatní součásti ZČU v rámci další veřejné zakázky.

2 Informace o zadavateli

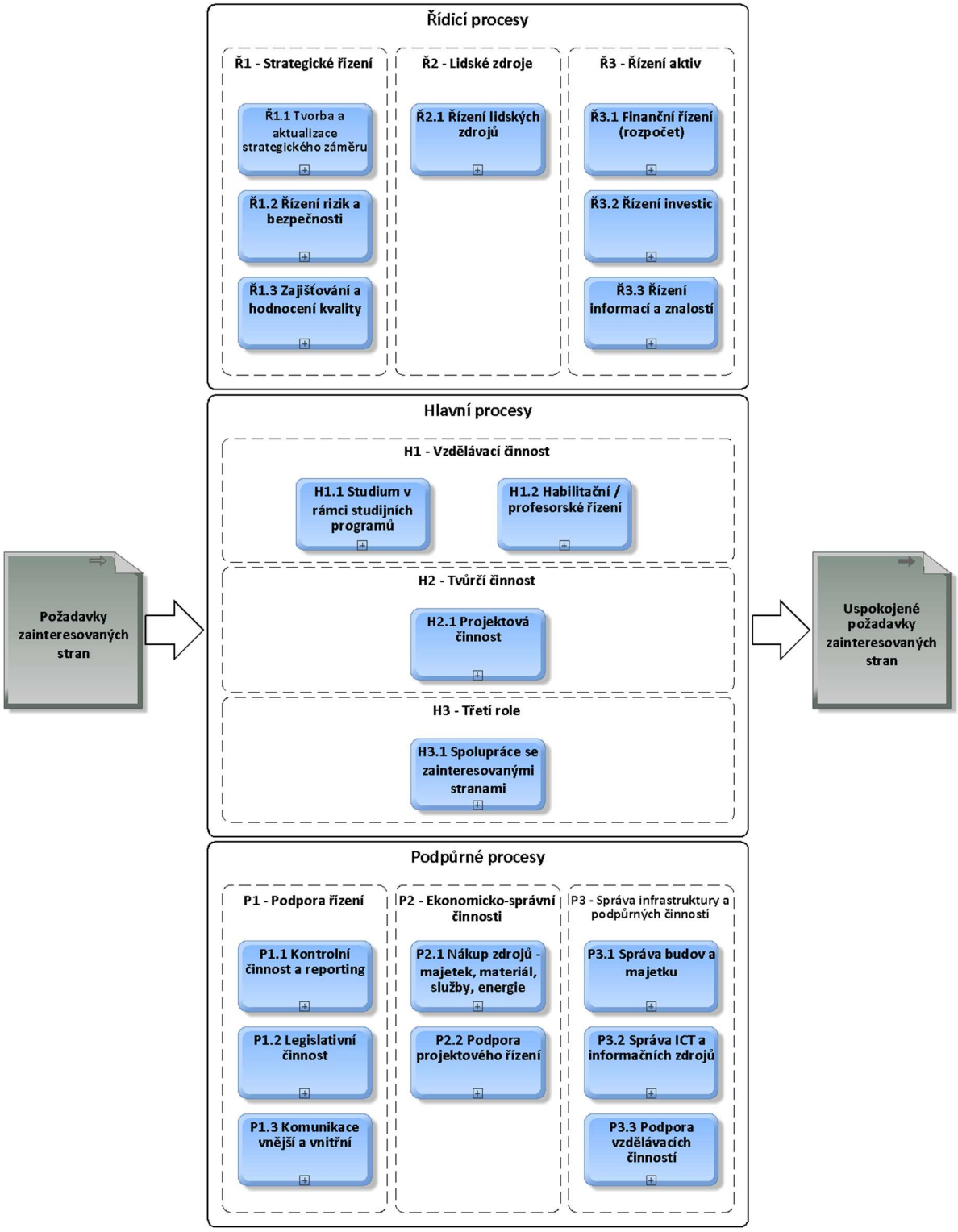
Fakulta elektrotechnická je jednou ze součástí Západočeské univerzity v Plzni. Fakulta poskytuje vysokoškolské vzdělávací činnost ve všech stupních studia (bakalářské, navazující magisterské, doktorské) a realizuje kompletní výzkumný řetězec od základního (teoretického) výzkumu až po vývoj funkčních vzorků a prototypů a jejich kompletní testování včetně smluvního výzkumu a doplňkové činnosti.

K 31. 12. 2022 měla fakulta 821 studentů a studentek (568 Bc., 148 NMgr., 105 Ph.D.), 193 přepočtených zaměstnanců (akademických, vědeckých a THP). Bližší informace jsou uvedeny ve výročních zprávách fakulty, které jsou zveřejněné na webových stránkách Dokumenty (zcu.cz).

Organizační struktura fakulty je popsána Organizačním řádem fakulty, který je uveden v příloze č. 1. Vybrané činnosti jsou zajišťovány centrálně pro všechny fakulty a součásti univerzity odbornými útvary ZČU (například vedení účetnictví, mzdová agenda, správa budov, služby v oblasti ICT, evidence majetku atd.).

Fakulta má v současné době zpracovanou procesní mapu viz obrázek níže. Dále jsou pro jednotlivé procesy vytvořeny modely, které jsou přístupné prostřednictvím interního procesního portálu univerzity.

Procesní mapa Fakulty elektrotechnické



3 Rámcový rozsah IS a integrace

Informační systém bude v rámci těchto zadávacích podmínek pokrývat uvedené oblasti prostřednictvím aplikačních komponent. Jejich podrobnější popis včetně požadovaných funkčností je v kapitole Funkční požadavky na jednotlivé aplikační komponenty.

Aplikační prvek	Význam	Typ dodávky
Informační systém	Nástroj pro vedení interních evidencí	1
Systém pro správu dokumentů	DMS s vazbou na IS	2
Systém pro tvorbu, správu a řízení procesů	Nástroj pro práci s procesy s vazbou na IS	2
Systém pro podporu interní spolupráce	Interní komunikační platforma	2
Nástroje na podporu řízení	Nástroje na zpracování získaných dat (MIS)	2

Typ dodávky**:**

1 – Aplikační komponenta je integrální součástí IS.

2 – Aplikační komponenta, která může být integrální součástí IS nebo může být řešena samostatným produktem (i třetí strany), který bude plně datově a funkčně integrovaný s jádrem IS a okolními systémy (EIS ZČU Magion, OBD, GaP, STAG atd.), což znamená zejména integraci v oblastech získávání a zápisu z a do IS, DMS a dalších.

3.1 Požadavky na integraci systémů a migraci dat

Požadavky na integraci se stávajícími systémy zadavatele budou předmětem Předimplementační analýzy, kterou je povinen provést dodavatel včetně případné analýzy migrace dat. IS musí poskytovat otevřené a zdokumentované integrační rozhraní (API), které umožní efektivní propojení systémů třetích stran vůči procesům a databázím obsaženým v informačním systému a jeho komponentám. Součástí nabídky musí být i minimální specifikace požadavků na zadavatele z pohledu nezbytné součinnosti pro integraci systémů a migrace dat. Integrační rozhraní je možné také realizovat s využitím dalšího systému na úrovni skryté transakční vrstvy. Jedná se především o migraci stávajících dat ze systému SVN (má být nahrazen novou DMS) a též případná migrace dat z aktuálně používaných MS Teams a Google Meet do nového systému pro podporu interní spolupráce. Pro spisovou službu je využíván Národní standard pro elektronické systémy spisové služby (dále jen NSESSS), který je publikován na stánkách MV ČR.

3.2 Požadavky na vytvoření standardizovaného komunikačního prostředí

IS musí umožňovat integraci s jinými systémy pomocí API. Jedná se především o systémy používané v rámci univerzity a též o komunikaci mezi jednotlivými aplikačními prvky dodávaného řešení. Informace k jednotlivým API stávajících IS ZČU (případně dalších způsobů konektivity) poskytne CIV ZČU v součinnosti s FEL ZČU v rámci předimplementační analýzy. Dodavatel musí poskytnout podporu ZČU/CIV/FEL nebo dodavatelům ZČU, kteří budou implementovat integraci s jinými systémy univerzity. Dodavatel může nabídnout vlastní řešení integrace s jiným konkrétním systémem. Pro spisovou službu bude využit NSESSS.

3.3 Základní integrační schéma

Jednotlivé aplikační prvky mají umožňovat komunikaci s ostatními systémy univerzity. Tato komunikace bude až na eSpis, přadně další IS ZČU jednosměrná. Předpokládá se možnost čerpání dat z účetního systému Magion (data personalistiky, agregovaná účetní data), systém studijní agendy STAG – data o studentech, předmětech…, systém pro správu „projektů“ GAP – údaje o projektu, rozpočty, systém pro evidenci výsledků výzkumu OBD – informace o výsledcích výzkumu. U aplikace eSpis se předpokládá vkládání dokumentů do univerzitní podatelny. Dále se předpokládá spolupráce s univerzitním poštovním serverem (webmail).

4 Požadavky na bezpečnost řešení

Jako nezbytnou součástí řešení musí dodavatel dodat procesní a technickou dokumentaci zejména v souladu s příslušnou legislativou vztahující se na celý předmět dodávky (zejména GDPR a zákona č. 181/2014 Sb., o kybernetické bezpečnosti). Je nutno dostát též předpisům v souvislosti s umístěním dat v cloudu.

4.1 Dokumentace provozních postupů

Dodavatel musí v rámci dodávky zpracovat dokumentaci, která musí zahrnovat tyto provozní postupy a skutečnosti:

- Spuštění a ukončení chodu systému a jeho aplikačních komponent.
- Instalace a konfigurace systému.
- Spuštění a konfigurace systému v tenkém klientu.
- Bezpečnostní dokumentaci:
    - bezpečnostní architektura,
    - implementované kontrolní mechanismy a bezpečnostní funkce,
    - privilegované a technické účty, privilegované role, matice rolí a neslučitelnost rolí,
    - bezpečnostní logy,
    - řízení přístupu včetně vzdáleného,
    - bezpečnostní nastavení ochrany DB a dat,
    - komunikační bezpečnost,
    - vzdálenou správu,
    - použité kryptografické nástroje, funkce a klíče,
    - verzování, kampaně, integrace, nezaměnitelnost apod.
- Popis datových rozhraní pro napojení na systémy 3. stran (API).
- Monitoring provozu systémů, aplikací a služeb.
- Postup identifikace, vyhodnocení, přijetí nápravných opatření a bezprodleného informování o kybernetických bezpečnostních incidentech souvisejících s poskytovaným řešením.
- Administrátorská a uživatelská dokumentace, metodiku a postupy způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy v půlročním intervalu. V případě zjištění nových rizik nebo změn stávajících rizik dodavatel informuje zadavatele bezodkladně.
- Zpracování a nakládání s informacemi.
- Vzájemné vztahy a vazby na jiné systémy.
- Postupy zálohování a obnova systému a dat ze záloh
- Restart nebo obnovení chodu systému po selhání, ošetření chybových stavů anebo mimořádných jevů.
- Podpora a eskalační kontakty v případě neočekávaných provozních nebo technických obtíží či bezpečnostních incidentů.

Dokumentaci musí dodavatel pravidelně aktualizovat při každé změně.

4.2 Popis oddělení prostředí pro vývoj, test a provoz dodávaného řešení, požadavky na testovací prostředí

Dodavatel musí zajistit z pohledu zajištění bezpečnosti prostředí:

- Testovací a provozní (produkční) prostředí musí být zcela oddělena v sítích a musí být podporována oddělenými stroji.
- Provozní servery nesmí obsahovat překladače a systémové utility, které nejsou nezbytné pro jejich správu nebo provoz.

- Testování a vývoj nových verzí systémů, aplikací i zařízení se nesmí provádět v provozním prostředí.
- Dodavatel musí dodržovat při vývoji svých produktů zásady SDL (Secure Development Lifecycle).
- Dodavatel musí vydefinovat v rámci Předimplementační analýzy požadavky na konfiguraci jednotlivých síťových a serverových prvků pro zajištění požadované bezpečnosti a funkčnosti.
- Pro potřebu školení uživatelů na nový informační systém a testování nově nasazovaných verzí informačních systémů musí dodavatel vytvořit testovací prostředí v dostatečném předstihu před pilotním provozem – duplicitní provoz.
- Dodavatel musí zajistit úvodní migraci dat i potřebné služby pro testování informačních systémů. Dodavatel musí testovací prostředí naplnit daty tak, aby bylo možné systém řádně otestovat. V rámci instalace nových verzí informačního systému bude zajištěna možnost pravidelně upgradovat provozovaná data, aplikace a komponenty.

4.3 Postup ověření identity uživatelů a řízení přístupových oprávnění

Zadavatel požaduje ověření identity (autentizace) v systému prostřednictvím centrálního univerzitního ověřování identity Shibboleth.

Z pohledu autorizace musí řešení podporovat hierarchizovatelné nastavení přístupových práv se stanovením rozsahu přístupu i stupně oprávnění manipulace se záznamem. Princip nastavování přístupových práv k jednotlivým uživatelům musí vycházet z definice libovolného množství uživatelských rolí a skupin, do kterých jsou jednotliví uživatelé přiřazováni v rámci identitního systému zadavatele. Je požadováno API pro automatizované nastavování rolí a práv. V rámci univerzity je používán systém MidPoint.

Dodavatel musí do dokumentace uvést detailní popis úrovně privilegovaných i neprivilegovaných přístupových oprávnění, resp. jednotlivých uživatelských rolí a to i ve vztahu k jednotlivým aplikačním komponentám.

4.4 Ochrana před škodlivým kódem

V rámci dodávaného řešení musí být zajištěna a popsána ochrana:

- komunikace mezi vnitřní sítí a vnější sítí,
- ochrana proti útokům z vnějších sítí včetně Threat Intelligence,
- ochrana serverů a sdílených datových úložišť,
- popis požadavků na zajištění bezpečnosti pracovních stanic (klientů).

4.5 Požadavky na logovací aparát

- logování pořízení záznamů v IS – uživatel, datum a čas,
- logování změny záznamů (včetně mazání) v IS – uživatel, datum a čas,
- logování nahlížení do záznamů v IS – uživatel, datum a čas,
- logování tisku záznamů v IS uživatel, datum a čas,
- logování veškerých operací prostřednictvím API – zdroj, datum, čas, operace, popis.

4.6 Zaznamenávání událostí, včetně návrhu jejich vyhodnocování

V rámci dodávaného řešení musí být realizováno zaznamenání minimálně následujících událostí:

- přihlášení a odhlášení uživatelů a administrátorů,
- činnosti provedené privilegovanými účty (administrátorské účty, systémové účty, technické účty apod.),
- činnosti vedoucí ke změně přístupových oprávnění (standardních i privilegovaných),

- neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů,
- zahájení a ukončení činností (včetně „pádů“ nebo selhání) jednotlivých komponent systému,
- činnosti spojené s přijímáním/odesíláním ze/do SW třetích stran (integrační logy),
- automatická varovná nebo chybová hlášení komponent systému,
- přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností,
- použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášen
- založení, změna, výmaz, čtení a tisk datových záznamů včetně času, uživatele a identifikace pracovní stanice, ze které byl úkon proveden (transakční protokol),
- trasování systémových změn na úrovni operačního systému, služeb.

Takto zaznamenané události musí být zpracovatelné (strukturované, strojově čitelné) nezávislým prostředkem pro ochranu získaných informací před neoprávněným čtením nebo změnou a pro další vyhodnocování (standardní rozhraní SIEM).

Dodavatel musí zajistit sledování průběhu bezpečnostních a kybernetických incidentů od počáteční analýzy, odstranění a zotavení až po uzavření prostřednictvím postupů/procesů SIR (Security Incident Response).

4.7 Aplikační bezpečnost

Dodavatel zajistí v rámci dodávaného řešení:

- trvalou ochranu aplikací a informací dostupných z vnější sítě před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou,
- trvalou ochranu transakcí před jejich nedokončením, nesprávným směrováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním.

4.8 Ochrana dat

Dodavatel zajistí v rámci dodávaného řešení následující.

Nastavení ochrany dat zpracovaných nebo uchovávaných v řešení, a to především osobních údajů nebo citlivých údajů, kdy bude kladen důraz na data dostupná z vnější sítě. Budou zohledněna rizika:

- neoprávněného přístupu,
- nedovolených činností nad rámec svých práv,
- popření provedených činností,
- kompromitace,
- porušení integrity dat,
- nedostupnosti dat,
- neautorizované změny.

Ochranu prováděných transakcí nebo změn dat:

- před jejich nedokončením,
- nesprávným směrováním,
- neautorizovanou změnou předávaného datového obsahu,
- kompromitací,
- neautorizovaným duplikováním nebo opakováním, a to v souladu s legislativními nebo normativními požadavky na ochranu dat, především GDPR.

4.9 Kryptografické prostředky

V případě využití kryptografických prostředků pro činnost dodávaného řešení, dodavatel zajistí použití kryptografických algoritmů a kryptografických. Kryptografické klíče musí být uloženy v bezpečném prostředí s možností auditu přístupu ke klíčům.

4.10Návrh a popis zabezpečení síťových služeb

Provedení propojení případných cloudových a on-premise komponent zajistí zadavatel. Komunikace mezi jednotlivými funkčními celky bude řízená na úrovni síťových služeb. Povolena bude pouze vzájemná komunikace, která je nezbytná pro funkci systému.

Přístup k vlastním službám, ke kterým se připojují uživatelé, bude chráněn prostřednictvím web application firewallu, který zajisti ochranu proti kybernetickým útokům. Vstupní, výstupní i vzájemná síťová komunikace mezi jednotlivými částmi systému bude monitorována viz podkapitola Monitoring níže.

4.11Monitoring

Zadavatel požaduje popis zdrojů, metrik a způsobů pro monitorování provozních stavů systému a jeho komponent včetně případných prahových hodnot (normální provoz/omezená funkčnost/nedostupnost). Systém rovněž musí zaznamenávat jednoznačná chybová hlášení.

Monitoring celého řešení se bude skládat z několika celků:

- Monitoring aplikace – zajistí dodavatel a poskytne přístup zadavateli. Cílem je získání pohledu na výkonnost celé aplikace a jejích součástí z pohledu uživatelské zkušenosti, zejména reakční doba komponent, korelace volání (tracing), neúspěšná volání a chybové stavy.
- Infrastrukturní monitoring – dodavatel v kooperaci se Zadavatelem. Využití monitorovacích prostředků Zadavatele, které mohou být doplněny o monitorovací systém dodavatele. Cílem je monitoring síťové propustnosti, dostupnosti služeb, výkonnostních parametrů atp. Aktuálně zadavatel používá systém Icinga (www.icinga.com).
- Zadavatel požaduje umožnit přístup k těmto datům prostřednictvím API za účelem vytváření analytických pohledů na tato data. Popis API bude součástí dokumentace.

5 Technické požadavky

Tato kapitola obsahuje přehled technických požadavků.

- Řešení musí být založeno na dostupných, moderních, ověřených technologiích a standardech s podporou budoucího vývoje, se kterými má dodavatel zkušenosti z jiných dodávek. Jsou požadovány reference na obdobná řešení dodavatele.
- Řešení musí mít optimalizované ovládání pro technologii dotykových obrazovek s ikonami pro rychlé a snadné ovládání.
- Řešení musí podporovat plnohodnotnou klávesnici a propojení na myš. Řešení musí umožnit zobrazení celé obrazovky pro jasnější interpretaci údajů. Řešení by mělo podporovat to, aby nejčastěji používané funkce byly dostupné klávesovou zkratkou a myší.
- Uživatelská část systému by měla být přístupná formou tenkého klienta, a to i na běžných mobilních zařízeních.
- Uživatelskou část systému lze spustit jak na stolních počítačích, tak na mobilních zařízeních s bezdrátovou technologií, jako je smartphone a přenosných tabletů. Zadavatel požaduje podporu všech běžných platforem operačních systémů, tedy: Windows 10/11 Enterprise/Pro/Education vždy minimálně v Current Branche for Business a LTSC (Long Term Service Channel), MacOS v nejnovější verzi a verzi -1, Android v nejnovější verzi a verzi až -3, iOS v nejnovější verzi a verzi -1, Linux alespoň v LTS verzích. Dále také podporu všech běžných webových prohlížečů v nejnovější verzi. Na všech zmíněných platformách je požadován tenký klient.
- Systém musí být zaveden ve vysoce redundantních konfiguracích a zajišťovat všechny úrovně zabezpečení.
- V případě výpadku službyje požadován reakční čas uvedený v Obchodních a platebních podmínkách, bod 8. 3.
- Je požadována výkonová škálovatelnost systému tak, aby bylo možno v případě dosažení mezních hodnot výkonových čítačů pružně zvýšit výkon.
- Systém musí umožnit ukládat naskenované dokumenty a propojovat je s příslušnými evidencemi.
- Systém musí mít možnost exportu dat do některého ze standardních datových formátů CSV, XLSX, JSON a OpenDocument (ODF) dle standardu OASIS Open Document Format, ISO/IEC 26300:2006, pro tvorbu reportů a statistik.

5.1 Obecné požadavky

- Systém musí v době ostrého provozu podporovat českou a anglickou jazykovou verzi a umožnit přepínání mezi nimi.
- Systém musí obsahovat funkci rychlého vyhledávání.

5.2 Uživatelské prostředí

- Aplikace/GUI musí mít responzivní design, tzn. nezávislost na rozlišení či orientaci zobrazovací jednotky či displeje bez vlivu na kvalitu a čitelnost zobrazení.
- Aplikace musí obsahovat interaktivní nápovědu.

5.3 Tiskové výstupy

Výstupy musí být v souladu a ve formátu předepsaného příslušnou legislativou a interními předpisy ZČU a FEL. Před tiskem musí systém umožnit náhled na tisk. Systém musí umožnit nastavení a vlastní vytváření tiskových předloh prostřednictvím integrovaného nástroje pro tvorbu sestav.

6 Funkční požadavky na jednotlivé aplikační komponenty

6.1 Informační systém

Evidence obchodních partnerů včetně podpory CRM

- Systém bude evidovat (nejen) obchodní partnery, jejich adresy a kontakty. Zároveň bude využit v dalších evidencích (projekty, smluvní výzkum...). V rámci evidence jsou též požadovány základní možnosti CRM jako zápisy ze schůzek, poznámky, hromadné pozvánky a rozesílání mailů. Dále systém umožní uložení průvodních dokumentů k obchodním partnerům jako jsou faktury, smlouvy a apod. Je požadováno napojení na univerzitní LDAP.

Personalistika a správa HR

- Evidence zaměstnanců a uchazečů s jejich základními údaji.
- Evidence školení zákonných i volitelných, jejich plánování a organizace, možnost vložení (importu) informací o externím školení včetně certifikátů a osvědčení.
- Evidence úvazků ve vztahu k projektům a zaměstnancům v návaznosti na systém MAGION, což obnáší proces změny úvazku formou požadavku a schvalovacího procesu. Úvazky musí být sledovány jak za osobu, tak za projekt. Jedna osoba může mít více pracovních úvazků ve vazbě na různé projekty a s různou pracovní náplní.
- Evidence pracovních náplní k jednotlivým úvazkům s možností jejich výstupu (popis pracovní náplně pro zaměstnance)
- Evidence pracovních cest včetně souvisejících procesů (plánování, přidělování prostředků, zápis o cestě) a tiskových výstupů
- Evidence dovolených včetně plánování a souvisejících procesů (žádost, schvalování)
- Plán individuálního rozvoje zaměstnanců s možností zařazení i externích školení
- Pravidelné individuální roční hodnocení zaměstnanců
- Výběrová řízení na zaměstnance včetně celého procesu (vyhlášení, ustavení komise, vyhodnocení uchazečů, vyhodnocení dle kritérií)
- Případné další HR procesy zjištěné během Předimplementační analýzy
- Import dat ze systému MAGION – informace o reálných mzdách ve vazbě na osoby a projekty

Řízení projektů

Evidence projektů v návaznosti na univerzitní systém GaP (schraňuje projekty od podání žádosti, přes schvalovací proces, proces řešení a následné udržitelnosti). V rámci implementace by měl systém podporovat vlastní řízení projektů v celém průběhu životního cyklu (viz výše). Zároveň je požadováno řešit následující související data:

- Seznam řešitelských týmů v návaznosti na personalistiku/hr a evidenci partnerů
- Plánování projektu, harmonogramy jednotlivých fází a jejich úkoly ideálně s možností využití nástroje pro plánování jako je MS Project
- Rozpočty a sledování jejich plnění v průběhu projektu
- Změnová řízení nad obsahem projektu
- Import účetních dat projektu ze systému MAGION, seznamy dokladů, roztříděná sumarizovaná data dle oblastí rozpočtů
- Evidence dokumentů souvisejících s projektem (odkaz na úložiště, odkazy do DMS)
- Evidence plánovaných výsledků (patenty, zprávy, publikace…) a sledování jejich plnění, jejich následná vazba na univerzitní evidenci OBD
- Nástroje pro vyhodnocení projektů (plnění harmonogramů a dalších ukazatelů)
- Sledování nákupů a nákladů

- Reportingové nástroje pro výstupy směrem k poskytovatelům projektů
- Reportingové nástroje pro spoluřešitele projektů
- Sledování vytížení (kapacit) laboratoří a přístrojového vybavení.

Řízení smluvního výzkumu a zakázek

Řízení smluvního výzkumu a běžných zakázek sleduje celý životní cyklus těchto procesů od přijetí poptávky, nabídky, zadání, řízení, sledování termínů, až po fakturaci a případnou evidenci výsledků (u smluvního výzkumu) včetně vazby na OBD. To vše opět ve vazbě na partnery a zaměstnance, dokumenty, případně informace získané z MAGIONu. Součástí může být harmonogram úkolů a dosažených výsledků výzkumu. Smluvní výzkum a zakázky jsou zjednodušenou podobou projektů.

Evidence přístrojů

V rámci evidence přístrojů se předpokládá seznam přístrojového vybavení s dodatečnými informacemi o:

- aktuálním umístění a případném přemisťování
- požadovaném a provedeném servisu
- požadovaných a provedených revizích včetně jejich plánování
- vedení provozních deníků
- informace o zápůjčkách ve vazbě na zaměstnance nebo partnery (externí zápůjčka)
- výstupní sestavy

Obecná evidence cizího majetku

V rámci činnosti běžně dochází k práci s cizím „vzorkem“ (testování, měření atd.) případně cizími přístroji, součástkami a podobně – obecně cizím majetkem. Je požadována dostatečně podrobná evidence tohoto majetku (popis, majitel, termíny) spojená s informací o projektu/zakázce které se týká, jeho umístění a zodpovědné osobě.

Metrologická evidence

Předpokládá se evidence měřidel využívaných v rámci vědecké činnosti a měřidel akreditované laboratoře. U měřidel je požadováno ukládání běžných informací (typ, umístnění správce, dodavatel, servis, aktuální stav) a informací o stavu kalibrace, požadovaných kalibracích a jejich historii. Vše opět s vazbou na dokumenty. Technicky může být součástí přístrojové evidence.

Evidence publikační činnosti, výsledků výzkumu, licencí a duševního vlastnictví

Evidence bude napojena na proces výsledků, tedy proces od záměru dosažení výsledku, jeho schvalování, dosažení, publikaci do univerzitního systému OBD. Dále pak možnost připojení nákladů na dosažení a případně udržování (patenty) a výnosů (prodej licence). K výsledkům mohou být též připojeny dokumenty. Předpokládá se vytvoření knowledgebase vycházející z této evidence (prohledávání uložených údajů i dokumentů)

Evidence požadavků na nákup

V rámci procesů budou evidovány požadavky na nákup. Tyto budou součástí procesu (schvalování, předání univerzitnímu oddělení, případné výběrové řízení, převzetí informace o uskutečnění), kde vlastní nákup řídí univerzita centrálně. Předání bude probíhat pravděpodobně podáním do eSpisu. Zpět z Magionu mohou být čerpána data o stavu nákupu.

Podpisová kniha

Tato evidence pravděpodobně bude nahrazena spisovou službou eSPIS nebo jinou platformou na úrovni ZČU, pokud nikoliv, požadované funkce jsou následující:

- Podepsat PDF dokument elektronicky.
- Použití kvalifikovaného certifikátu.
- Umožnit hromadný podpis dokumentů (za určitých podmínek).
- Provedení podpisu zalogovat do podpisové knihy (kdo, kdy, co a čím podepsal).
- Řešit platnost podpisů (ověření i po vypršení platnosti podpisového certifikátu).
- Umožnit propojení se správou procesů (podepsání dokumentu může být součástí procesu).

6.2 Další obecné požadavky na informační systém

Komunikace s ostatními systémy univerzity a nové platformy:

- Předpokládá se v omezeném rozsahu komunikace s univerzitním systémem MAGION. Tuto implementovat minimálně jednosměrně s ohledem na potřebu získávání dat pro řízení projektů a manažerské výstupy (zejména náklady a výnosy pro jednotlivé zakázky, údaje z personalistiky a majetku).
- Import dat z IS/STAG (studenti, kvalifikační práce, rozvrhové akce)
- Komunikace s OBD (informace o stavu výsledků a další)
- Komunikace s GaP (informace o projektech)
- Komunikace se spisovou službou eSpis (oběh dokumentů dle spisového řádu ZČU)
- Vazba na podporu procesů
- Případně další agregovaná data dostupná v datovém skladu, případně pomocí datových pump

Informační systém má uživatelsky sloužit primárně pro zaměstnance fakulty k podpoře jejich procesů. Jako uživatelský klient se předpokládá tenký klient (webový prohlížeč) s přístupem prostřednictvím univerzitního ověřování.

Požadovanou vlastností je možnost vlastního rozšiřování stávajících evidencí, případně doplnění nových vlastními silami (vyškolený správce). Dále pak možnost tvorby vlastních výstupů formou generovaných sestav v integrovaném návrháři sestav. Výstupy by mělo být možno směrovat na tisk, do PDF (případně i podepsaného dokumentu), případně do WORDu či EXCELu, i ve formě dále zpracovatelných dat – exporty XML, JSON. V rámci integrace dokumentů do spisové služby musí být předávány dokumenty ve formátu PDF s textovou vrstvou (PDF A3)-

Akce uživatelů i interakce s ostatními systémy má být logována. Uživatelům má být možno přiřazovat přístup k jednotlivým oblastem a evidencím s různou měrou oprávnění (náhled, zakládání, úpravy, mazání atd.)

Systém má mít možnost být součástí procesů vytvářených systémem pro správu procesů (data ze systému jsou použita v procesech, data z procesů mohou být vkládána do systému).

6.3 Systém pro správu dokumentů

Je požadován systém správy dokumentů, který umožní následující operace s dokumenty:

- Vkládání, sdílení a archivace dokumentů v běžných formátech.
- Organizace do adresářových struktur.
- Spolupráce nad dokumenty (společnou práci více uživatelů nad dokumentem v souběhu i variantu držení a uvolnění dokumentu).

- Sledování interakce s dokumentem.
- Možnost nastavení přístupových práv na úrovni adresářů i jednotlivých dokumentů a to vůči skupinám uživatelů i jednotlivým uživatelům.
- Možnost verzování dokumentu a sledování jeho historie.
- Interní / cloudové uložiště splňující zákonné požadavky pro organizaci tohoto typu.
- Možnost připojit se na systém správcem souborů.
- Možnost vytvoření odkazu na dokument např. do mailu, případně do informačního systému, nebo systému na správu procesů.
- Možnost napojení jako zdrojové / cílové místo pro proces.
- Možnost procesu k seznámení se s dokumentem s protokolováním toho, že byl dokument opravdu „přečten“ a kdy se tak stalo (aktuálně se pro tento proces používá MOODLE).
- Navázání oběhu dokumentů, včetně archivace a skartace na spisovou službu ZČU e-Spis.

6.4 Systém pro tvorbu, správu a řízení procesů (workflow)

V této části systému se předpokládá tvorba, správa a řízení procesů. Procesy by měly být postaveny z jednotlivých stavebních kamenů sloužících pro interakci s uživateli nebo okolními systémy. Jednotlivé kroky budou definovány v návrháři procesu (nejlépe grafický, ne nutně tenký klient, předpokládá se tvorba vyškoleným správcem) s možností vytvořit například vlastní masku pro vstup dat od uživatele do procesu. Každý proces by měl mít vlastní definovatelnou datovou strukturu s možností zápisu do informačního systému, nebo do jiných míst.

Dále by pak mělo být možno sledovat který proces v jakém stádiu probíhá a kdo se jej účastní. Veškeré interakce mají být logovány. Uživatelské prostředí pro interakci s procesem musí fungovat v tenkém klientu.
Jako jednotlivé stavební kameny by měly být dostupné:

- Vstupní formulář pro data od uživatele – jednoduchý vstupní formulář implementačně upravitelný co do dat, která budou zadána nebo zobrazena, tak vlastní podobu vstupního formuláře (například maska pro žádost o dovolenou bude potřebovat jinou masku než primární vstup požadavku na nákup). Vstupní formuláře by měly být přístupné opět z webového prohlížeče.
- Načtení dat z externího systému, například z projektu, seznamu partnerů, personalistiky – tedy například výběr uživatele, kterému se předá proces v dalším kroku (vedoucí, jiný nadřízený, referent nákupu…), nebo data potřebná ke zobrazení v některém dalším kroku či vyplnění polí formuláře.
- Vygenerování výstupu na základě dat procesu (například vytištěná žádost, vytištěné roční hodnocení…) a případně jeho posun v procesu (třeba k podpisu).
- Schvalovací proces s jedním uživatelem. Uživatel dostane pokyn schválit aktuální stav. K tomu musí mít možnost vidět v čitelné formě data procesu který schvaluje. (například tedy pokud schvaluje požadavek na nákup měl by vidět kdo a co chce nakoupit, případně i další parametry požadavku). Měl by též mít prostor schválit nebo neschválit s vyjádřením.
- Schvalovací proces s více uživateli obdobně jako výše s tím že se může jednat o situaci, kdy je nutno více úrovní schválení.
- Hlasovací proces – hlasování nad daty procesu.
- Podpisový proces – součástí může být dokument, nebo seznam dokumentů s požadavkem na podpis.
- Zápis dat do informačního systému (posbíraná data procesu jsou zapsána do příslušných evidencí a následně využita například k vygenerování tiskového výstupu).

- Výstup do XML, JSON nebo jiného formátu pro výměnu dat v definované podobě (podklad pro volání webové služby nebo další).
- Výstup dokumentu do systému pro správu dokumentů.
- Výstup dokumentu do spisové služby eSPIS.
- Výstup do mailu, či jiné komunikační platformy.
- Větvení procesu na základě dat.
- Možnost reakce na „externí“ podnět (ne ruční vstup od uživatele) – například termín, změnu stavu dokladu v systému.

V rámci tohoto systému budou zpracovávány a řízeny například následující procesy (a jejich možný průběh):

- Žádost o dovolenou (zadání žádosti, schvalovací proces, odeslání v požadovaném formátu personálnímu oddělení k zapsání do MAGIONu, při vyznačení dovolené ve sdíleném kalendáři).
- Obdobný proces s pracovní cestou (žádost, schvalovací proces, předání účtárně, výstup do kalendáře).
- Změny úvazků – zadání žádosti o změnu úvazku u pracovníka, předání mzdovému oddělení k zápisu do MAGIONu, po dokončení provedení změny u příslušného úvazku v informačním systému fakulty.
- Přidělování odměn – vyhlášení sběru návrhů, po ukončení sběru vícestupňové schvalování, přidělování zdrojů a následně předání do MAGIONu.
- Roční hodnocení zaměstnance – zahájení hodnocení, zadání sebehodnocení, import dostupných vstupních dat o osobě z personalistiky, postoupení k hodnocení schvalovatelům, po schválení zápis informací zpět do systému a vygenerování příslušné sestavy, uložení sestavy do dokumentové databáze ve vazbě na osobu.
- Požadavek na nákup – zapsání požadavku na nákup, schválení požadavku, předání ve formě vygenerované sestavy univerzitnímu oddělení nákupu.
- Práce s výsledky výzkumu – zadání záměru dosažení výsledku, schválení, po vypracování výsledku jeho předání s dokumentací ke zpracování do OBD.
- Žádosti o stipendium.
- Žádosti o nostrifikaci.
- Procesy týkající se doktorandského studia a to zejména:
    - Příjímací řízení.
    - Zápis.
    - Zkoušení.
    - Návrhy a schvalování témat.
    - Výroční zprávy.
    - Obhajoba DPP.

Stavy jednotlivých vláken procesů by měl být sledován a dostupný z přehledových dashboardů uživatele (chci vidět procesy, které vlastním a místa, kde je vyžadována moje interakce (doplnění, schválení, podpis), přidělené úkoly, úkoly, kde jsem zadavatelem…)

6.5 Systém pro podporu interní spolupráce

Aktuálně týmy spolupracují nad řešeními od MS a Google. V rámci toho dochází i ke sdílení dokumentů v rámci teamů, nicméně nejsou dostupné jinak než skrz aplikaci komunikační SW používaného řešení.

Je požadována komunikační platforma na které bude možno sdílet dokumenty na vyhovujícím úložišti, nejlépe takovém, které je možno procházet pomocí souborového manažera. V rámci komunikační platformy se mimo vlastních schůzek využívají:

- Podpora online schůzek, možnost vytváření zápisů z jednání, ideálně s možností propisu do CRM části informačního systému
- Distribuce zpráv a oznámení (asi realizovatelné i pomocí procesů)
- Pozvánky – rozeslání poznámek – ideálně například na základě seznamů řešitelů u projektů, případně jiných seznamů
- Hlasování – obdobně jako u správce procesů (případně shodné)
- Sdílené kalendáře – osobní, teamové, pro laboratoře a zasedačky, prostředky – s možností synchronizace aktuálních kalendářů pracovišť (jejich rozvrh je pak vidět na tabletech u vchodu).
- Notifikace na mobilní zařízení (GCal)
- Přímá spolupráce nad sdílenými dokumenty

6.6 Nástroje na podporu řízení

Je požadována implementace nástrojů na podporu řízení a to zejména:

- Uživatelské dashboardy s přehledy úkolů a procesů.
- Parametrizovaný sběr dat pro BI a jejich následnou analýzu.
- Tvorba vlastních ukazatelů a výkazů.
- Plánování finančních zdrojů.
- Sledování ekonomických dat (data čerpána z MAGIONu v definované podobě)
- Finanční analýzy a reporting.
- Tvorba analýz a plnění strategických cílů.
- Tvorba analýz z jednotlivých procesů.
- Hodnocení rizik, plánování a realizace opatření na základě získaných dat.

Většinově se bude jednat o zpracování průřezů daty zpracovanými informačním systémem a importovanými výtahy dat ze systémů univerzity.

6.7 Další informace a požadavky

Komplex výše uvedených systémů má být využíván širokou škálou uživatelů FEL, odhadem primárně cca 250 zaměstnanců a cca 2000 studentů. Je nutno počítat s možností růstu. Ověřování uživatelů je řešeno centrálně (Shibboleth) na úrovni univerzity, předpokládá se využití tohoto ověření implementovanými systémy.

Na klientské straně je ideálně běžná „kancelářská stanice“ vybavená prohlížečem a MS-Office (příp. Microsoft 365 nebo LibreOffice). Běžné operace jako například zadání jednoduchých dat do webového rozhraní probíhajícího procesu by mělo být umožněno z prohlížeče v mobilním zařízení (chytrý telefon, tablet). Pro správcovské operace (návrhy procesů, používání návrháře sestav) se předpokládá využití běžného PC.

Je požadováno udržení technologické kompatibility se stávajícími systémy v dlouhodobém horizontu. Pro interní úpravy a přizpůsobování systému se předpokládá vyškolení interního správce (správců). Měl by být schopen rozšiřovat, upravovat případně vytvářet nové evidence v informačním systému.

Dále by měl správce systémů mít tyto možnosti související s úpravami, customizací a nastavení, zejména:

- vytváření libovolných rolí a modifikace u nich oprávnění přístupu k datům,
- úprava číselníků, které informační systém využívá aplikačních komponentách popsaných v kapitole 6.1,
- provádění úpravy struktury jednotlivých aplikačních komponent informačního systému samostatně bez zásahu dodavatele systému,

- změny název jednotlivých polí v aplikačních komponentách podle terminologie používané v prostředí ZČU,
- úprava adresářové struktury pro ukládání dokumentů a přidělovat k adresářům oprávnění,
- úprava vstupního formuláře do workflow samostatně bez zásahu dodavatele systému (viz bod 6.4),
- úprava schvalovatele pro workflow (viz bod 6.4),
- vytváření tiskové formuláře bez zásahu dodavatele systému,
- správce, případně uživatelé mohou samostatně vytvářet a zadávat notifikace a upozornění na různé události bez zásahu dodavatele systému,
- připojení libovolného vzdáleného úložiště dokumentů bez zásahu dodavatele systému,
- rozlišování a vytváření nové, vlastní aplikační komponenty nad rámec poptávaných komponent v seznamu 6.1. dodaných v rámci projektu.

Nad daty informačního systému, případně nad importovanými daty, vytvářet či upravovat výstupní sestavy. V rámci správce procesů pak vytvářet a upravovat jednotlivé procesy včetně jejich napojení na informační systém a případné přípravy vstupních formulářů. Zároveň se bude starat o místní podporu uživatelů.

Je požadováno důsledné zabezpečení systému vzhledem k předpokladu obsahu citlivých dat. Zabezpečení a funkce musí odpovídat GDPR a ostatním platným standardům.

Hardwarové a softwarové požadavky systému je nutno konzultovat s CIV ZČU.

6.8 Související systémy

- MAGION – univerzitní účetní SW – obsahuje účetní data, data mzdového účetnictví
  OBD – nástroj na evidenci vědeckých výsledků
  IS/STAG – studijní agenda – obsahuje data studentů
  GaP – správa projektů a grantů
- Webmail – poštovní a kalendářová služba ZČU
- MidPoint – identity management, systém pro centrální správu uživatelů, jako jedno z rozhraní poskytuje LDAP
- Icinga - centrální monitorovací systém
- Espis – spisová služba ZČU

7 Implementace

7.1 Požadavky na dokumentaci k systému

1. Zadavatel požaduje dodání kompletní dokumentace k systému. Jedná se o:

- Bezpečnostní dokumentaci
- Uživatelskou příručku
- Administrátorskou dokumentaci
- Technickou dokumentaci popisující integrační vazby pro rozhraní
- Technickou dokumentaci všech zahrnutých API.

2. Dodavatel je povinen tyto dokumenty udržovat aktuální bezodkladně po výskytu změny na produkčním prostředí systému.

3. Dodavatel s každou novou verzí předá zadavateli v elektronické podobě odpovídající uživatelské příručky i technologické postupy a popisy rozhraní na ostatní informační systémy.

4. Dokumentace musí být verzována včetně popisu změn vůči verzím předchozím.

7.2 Služby týkající se implementace

1. Před zahájením předimplementační analýzy dodavatel vypracuje Iniciační dokument projektu, který musí být odsouhlasen Zadavatelem. Iniciační dokumentace projektu bude minimálně obsahovat:

- Základní ustanovení
- Cíle projektu
- Rozsah projektu
- Plán projektu s přednastavenými milníky a kontrolními body
- Způsob řízení a organizace projektu
- Proces akceptace. Dodavatel je povinen připravit podklady pro akceptaci dodaného řešení
- Strategii řízení kvality, dodavatel bude garantovat provádění kontroly kvality po celou dobu životnosti projektu a povede registr kvality
- Strategii řízení konfigurace a povede registr konfigurace
- Strategii komunikace

2. Iniciační dokumentace bude pokrývat všechny fáze životního cyklu projektu, přechod mezi fázemi i upravovat výstupy projektu. Iniciační dokumentace projektu bude v průběhu projektu aktualizovaná, a to vzhledem k potřebám plnění dodávky díla, a to dohodou obou stran. Dodavatel bude spravovat projektové dokumenty, které budou uloženy v úložišti zadavatele. Požadovaná součinnost zadavatele v rámci analýzy bude dodavatelem předána před zahájením samostatné Předimplementační analýzy.

Na základě provedené Předimplementační analýzy bude implementace provedena v následujícím pořadí:

1. Technické instalace.
2. Konfigurace a úpravy aplikace.
3. Konfigurace a úpravy integračního rozhraní.
4. Testování (migrace dat, beta testy, integrační testy, systémové testy, funkční testy (FAT), simulace výpadků HW).
5. Provedení penetračních testů celého řešení včetně testů aplikační vrstvy v souladu s normami ČSN ISO/IEC TR 13335 a ISO/IEC 27002:2022 dle obecně uznávané metodiky (např. OSSTMM, OWASP, NIST apod.).
6. Provedení zátěžových testů – souběžná práce minimálně 30 % uživatelů.
7. Proškolení klíčových uživatelů a správců systému na vlastních zmigrovaných datech.
8. Akceptační testy pro pilotní provoz.

9. Nasazení na produkční prostředí – pro pilotní provoz.
10. Definice a nastavení přístupových práv.
11. Pilotní provoz.
12. Vyhodnocení pilotního provozu – incidenty, jejich řešení, následné kroky a doporučení.
13. Akceptační testy zadavatele.
14. Školení a řízení změn.
15. Postupný roll-out.
16. Uvedení do ostrého provozu.
17. Finální akceptace.

7.3 Požadavky na zpracování předimplementační analýzy

Práce dodavatele na vytvoření Předimplementační analýzy budou zahájeny neprodleně v termínu stanoveném Rámcovým harmonogramem z platné smlouvy. Předimplementační analýza naváže a detailně doplní zjištění předložená zadavatelem v rámci zadávacího řízení.

Výstupem analýzy bude mimo jiné vytvoření protokolů a procesů, které budou implementovány do systému. Zadavatel požaduje, aby základním pramenem pro tvorbu těchto protokolů a procesů byly mezinárodně uznávané standardy, zkušenosti dodavatele a další.

Kompletní výčet standardů (klasifikačních, procesů/protokolů), které budou využity pro zpracování systémové analýzy dle bodů výše, bude definován ve spolupráci dodavatele a zadavatele v rámci předimplementační analýzy. Předimplementační analýza (resp. komunikace se zadavatelem, výstupy, dokumenty atd.) bude realizována v českém jazyce. Zadavatel požaduje na dodavateli zpracování analýzy standardních procesů a procesního modelu FEL založeného na standardních procesech dodávaného řešení, který bude obsahovat:

- Analýzu procesů a souvisejících procesů FEL tak, aby byla zajištěna jejich realizovatelnost v rámci dodávaného řešení. Bude popsán každý implementovaný proces a forma jeho zpracování v dodávaném řešení.
- Analýzu funkčnosti a obsahu systému tak aby pokryl veškeré funkční a technické požadavky na dodávané řešení popsané v tomto dokumentu.
- Analýzy požadavků na integraci stávajících systémů a detailní analýza rozhraní (viz bod Související systémy tohoto dokumentu).
- Analýzy migrace dat a určení funkcionalit informačních systémů, jež budou nahrazeny.
- Analýzy prvků a služeb cloudu, které budou využité k vystavení infrastruktury řešení.
- Popis technického řešení včetně zajištění redundance provozu, zálohování, řešení výpadků a zajištění náhradního provozu.
- Specifikaci požadavků na licence.
- Návrh a popis akceptačních testů projektu.
- Plán roll-outu. Roll-out musí být postupný po jednotlivých pracovištích.
- Plán školení pro uživatele, správce a implementátory systému (úpravy informačního systému, tvorba a úpravy evidencí, tvorba procesů v návrháři procesů a jejich nasazení, tvorba sestav, správa všech jednotlivých částí systému, práce s uživateli a oprávněními atd.).

Výše uvedené body slouží zároveň jako akceptační kritéria pro Předimplementační analýzu.

Pro zpracování Předimplementační analýzy zadavatel poskytne dodavateli součinnost v zajištění odborných konzultací. Součástí nabídky musí být i minimální specifikace požadavků na zadavatele z pohledu nezbytné součinnosti pro zpracování Předimplementační analýzy.

Akceptační proces Iniciační dokumentace a Předimplementační analýzy bude realizován následujícím způsobem:

- Bude vytvořena akceptační komise (členové projektového týmu, vedení FEL a CIV)
- Bude posouzena úplnost zpracovaného dokumentu (dle požadavků objednatele)
- Bude posouzen obsah dokumentu, zda lze projekt (následující etapu) na základě dokumentu realizovat
- Bude zpracován seznam připomínek a odevzdán dodavateli
- Dodavatel zapracuje připomínky
- Bude posouzeno zapracování připomínek

Závěr akceptační komise:

- Akceptováno
- Akceptováno s výhradami
- Neakceptováno

Pokud nebudou výstupy akceptovány, dojde k odstoupení od smlouvy.

7.4 Požadavky na technologické vybavení pro provoz navrženého IS

1. FEL požaduje zajištění provozu v prostředí cloudu. Součástí nabídky bude i cena cloudových služeb na dobu 5 let.
2. Veškeré technické vybavení bude koordinováno s CIV
3. FEL požaduje zajištění testovacího prostředí v cloudu.
4.
5. Vývojové prostředí si zajistí Dodavatel sám.
6. Dodavatel v rámci předimplementační analýzy vyspecifikuje požadavky na technologickou infrastrukturu (požadavky na servery, síťové prvky, parametry úložiště) na instalaci a provoz IS, přičemž poptávaný aplikační software musí zohledňovat minimální požadavky na technickou dostupnost systému, požadavky na výkonnostní škálovatelnost systému, obnovu systému, zálohování systému a další požadavky vyspecifikované níže.
7. Dodavatel musí v rámci předimplementační analýzy předložit návrh architektury infrastruktury pro dodávané řešení a jeho začlenění do stávající infrastruktury Zadavatele.
8. Dodavatel v rámci nabídky vyspecifikuje požadavky na všechny licence.

7.5 Minimální požadavky na technickou dostupnost systému (business continuity)

Dodávané řešení musí obsahovat kombinaci prvků vysoké dostupnosti a dále ochranu před výpadkem. Vysoká dostupnost bude řešena ve spolupráci s CIV. Výpadek zóny dostupnosti tak nesmí vyvolat datovou ztrátu. Řešení výpadku musí být plně automatizované.

7.6 Požadavky na výkonnostní škálovatelnost systému

V případě naplnění mezní hodnoty výkonových čítačů, jako jsou např. vytížení CPU, paměti, latence systému atd., musí být možné zajistit bez výpadku systému škálování prostředí. V případě aplikační a prezentační vrstvy zadavatel preferuje scale-out řešení, tedy možnost zvýšení výkonu přidáním dalších uzlů a jejich začlenění do balancovaného clusteru.

1. Alternativně je možné použít scale-up řešení ve formě navýšením výkonu jednotlivých node tvořící prostředí tak, aby při této operaci nedošlo k přerušení provozu (například změnou velikosti záložního serveru a následné přepnutí provozu na tento server). Stejný scénář platí pro databázovou vrstvu.
2. Propojení s cloudovým prostředím a prostředky pro IS bude zajišťovat privátní VPN ze sítě zadavatele přímo do cloudového prostředí s dostatečnou rychlostí a s možností navýšení v případě potřeby.

3. Zadavatel má k dispozici internetové připojení 2*100Gb/s up/down. Páteřní síť LAN komunikuje 40/100 Gb/s, koncové stanice jsou připojeny 1 Gb/s.
4. Zadavatel poskytne nutné serverové prostředky ke zprovoznění celého řešení, které bude mít dodavatel kompletně pod správou a bude po odsouhlasení zadavatelem zajišťovat updatování operačního systému vždy na odsouhlasenou verzi, kompletní správu operačního systému a veškerých instalovaných aplikací. Dodavatel může dodatečně použít i vlastní prostředky monitoringu a realizace správy updatů.
5. Jakékoliv zásahy do HW řešení dodavatel bude provádět pouze s koordinací se zadavatelem a naopak (update firmware, servisní zásahy na vadné díly atp.).
6. Dodavateli bude umožněn nezbytný vzdálený přístup na veškeré prostředky spojené s instalací IS a to přímo na konkrétní prostředky pomocí VPN.

7.7 Návrh a popis zálohování, obnovy a kontinuity navrhovaného řešení

Zadavatel požaduje, aby dodavatel vypracoval finální dokumentaci včetně popisu postupu pro obnovu částí nebo celého systému, vypracování plánů záloh (včetně způsobu ukládání medií se zálohami) a návrhu disaster recovery plánů a souvisejících testů (co, jak často, do jaké úrovně, apod.). Vysoká dostupnost a disaster recovery bude využívat synchronizační prostředky popsané výše, ale systém musí obsahovat i zálohu pro případ poškození dat způsobeném například malware nebo chybou aplikace. Zadavatel také požaduje možnost přesunu celého řešení do jiné cloudové platformy nebo na vlastní servery v souladu s připraveným Exit plánem. Zadavatel má následující minimální požadavky z pohledu retence a četnosti záloh:

Záloha databáze:

- Plná záloha každých 7 dní.
- Inkrementální záloha každý den.
- Záloha logů každou hodinu.

Retence záloh:

- Logy po dobu mezi inkrementálními zálohami.
- Inkrementální denní zálohy + plné zálohy po dobu 1 měsíce.
- Týdenní plné zálohy po dobu 6 měsíců.
- Měsíční zálohy po dobu 3 let.
- Záloha aplikačních systémů
- Záloha každý den nebo po každé významné změně aplikační verze nebo velkého zásahu do nastavení.

Retence záloh:

- Denní zálohy po dobu 1 týdne.
- Týdenní zálohy po dobu 6 měsíců.
- Měsíční zálohy po dobu 3 let

Internetový prohlížeč

IS musí podporovat všechny běžné webové prohlížeče v nejnovější verzi (včetně mobilních zařízení) tedy: MS Edge, Google Chrome, Mozilla FireFox.

Stanice

Zadavatel předpokládá uživatelský provoz v tenkém klientu ve výše uvedených prohlížečích. U nástrojů správy systému případně na úrovni aplikací instalovaných MS Windows, Mac OS či GNU/Linux. Případné aplikace či jejich updaty budou dodávány v podobě instalačních balíčků

8 Zajištění kvality dodávek

Dodavatel se zavazuje ověřit kvalitu dodávek před jejich předáním z hlediska souladu postupů s metodikou, standardy, obecně závaznými právními předpisy a též provedením interního testování, a to nejméně v tomto rozsahu:

1. Testování funkcionality nových a měněných modulů.
2. Ověření funkčnosti komunikace s externími systémy (je-li předmětem změny).
3. Ověření instalace včetně kontroly správnosti a úplnosti sestavení dodávky.
4. Ověření bezpečnosti webových služeb a aplikací.
5. Ověření, zda výstup vyhovuje z hlediska výkonnosti a dostatečných odezev systému.

Dodavatel se zavazuje, že:

1. Dodá prohlášení/protokol o provedení interního testování a jeho výsledky v elektronické podobě, a to jako součást předání každého výstupu k testování zadavateli.
2. Dodá testovací scénáře pro testování výstupu na straně zadavatele, a to pro uživatelské akceptační testy.
3. Po dodání výstupu a po jeho instalaci do prostředí zadavatele provede integrační testy (pokud jsou nutné), vybrané průřezové testy a výkonnostní testy, které zaručí, že je možné zahájit uživatelské akceptační testování prováděné zadavatelem. V rámci akceptačního testování zadavatelem musí být prověřeno (mimo ostatních akceptačních kritérií), že systém splňuje kritéria potřebné odezvy. Odezvou systému se rozumí doba od zadání akce uživatelem v uživatelském rozhraní systému do úspěšného dokončení zadané akce systémem.
4. Zadavatel požaduje, aby systém v produkčním prostředí poskytoval minimální rychlost odezvy (viz Tabulka 1):

Tabulka 1: Požadovaná rychlost odezvy

Typ uživatelské akce	Parametry rychlosti odezvy
Běžná akce – jednoduché vyhledávání (do 5 vyhledávacích parametrů), otevření záznamu, založení záznamu, editace záznamu, výběr hodnot z číselníku, mazání záznamu atp.	• do 3 sekundy min. v 80 % případů
	• do 5 sekundy min. v 20 % případů
Náročnější akce – složitější vyhledávání (více než 5 vyhledávacích parametrů), tvorba komplexních výstupních sestav, dávková zpracování atp.	• do 7 sekund min. v 80 % případů
	• do 10 sekund min. v 20 % případů

Dodržení požadavku na rychlost odezvy bude jednorázově ověřeno v rámci zátěžových testů při testování dodávané služby.

1. Všechny chyby odhalené testováním budou dokumentovány a klasifikovány podle jejich závažnosti.
2. Všechny opravy chyb zjištěných během testování budou jednoznačným a pro zadavatele dostupným způsobem evidovány a dokumentovány.
3. Všechny přechodové stavy v testovacích cyklech budou dokumentovány.
4. Osoby provádějící testování se nebudou podílet na vývoji oblasti, kterou testují.
5. Umožní zadavateli ověřit řešení/modifikaci pilotním provozem na vybraných pracovištích či si k akceptačnímu řízení a k akceptačnímu testování přizvat externího konzultanta.
6. Dodavatel je povinen prokazatelným způsobem evidovat uživatel zjištěných chyb (např. ve formě samostatné položky v helpdesku nebo jiné dokumentaci přístupné oběma stranám) tak, aby se na tomto základě mohl výskyt chyb průběžně sledovat a po ukončení testování

sumarizovat a po odsouhlasení zadavatelem použít pro následné stanovení sankce za chyby v předmětu plnění.

8.1 Servis a podpora

Zadavatel bude mít podporu první úrovně plně ve své kompetenci, s řízenou distribucí požadavků na interní support, nebo podporu dodavatele.

8.2 Popis rozsahu služby

Obsahem služby je poskytování servisní podpory, zejména poskytování servisní podpory pro řešení incidentů a požadavků produktivního provozu. Dodavatel musí poskytovat podporu v těchto oblastech:

1. Podpora a údržba aplikace IS
2. Systémová podpora IS
3. Služby podpory provozu IS
4. Služby na vyžádání

8.3 Podpora a údržba aplikace IS

1. Garance funkčnosti – Dodavatel se zavazuje po dobu platnosti této podpory zajišťovat opravu zjištěných chyb v programovém kódu formou aktuálně vydávaných softwarových opravných kódů (ozn. jako hot-fix nebo patch).
2. Garance aktuálnosti a rozvoje dodaného SW – Dodavatel se zavazuje po dobu platnosti této podpory rozvíjet a poskytovat zadavateli updaty a upgrady tohoto IS, které byly výrobcem uvolněny na trh. Dodavatel zajistí, aby IS byl vždy ve verzi, která je podporována ze strany výrobce SW. Dodavatel musí zajistit aktuálnost IS na všech aktivních i neaktivních nodech serverové části systému. Zároveň musí dodavatel zajistit dostupnost aktualizací pro případné součásti řešení (např. aplikace pro správu) na klientské straně a zajistit případné upozornění na nutnost jejich provedení.
3. Garance bezpečnosti ASW – Dodavatel se zavazuje po dobu platnosti této podpory řešit bezpečnostní chyby, hackerské útoky, zjištěné zranitelnosti.
4. Garance legislativních updatů – Dodavatel se zavazuje provádět úpravy IS tak, aby tento pracoval v souladu s platnými právními předpisy ČR a EU.
5. Úpravy, které vyplynou ze vzniku zcela nových předpisů, budou řešeny v rámci rozvoje systému. Termínem „legislativní požadavky“ se rozumí požadavky dané zákonem nebo podzákonnou právní normou uveřejněnými ve sbírce zákonů ČR a legislativy EU. Úprava IS bude provedena při každé změně právních předpisů, která se bude dotýkat funkcí IS. Lhůta k nasazení do ostrého provozu včetně jejich otestování sjednána nejpozději ke dni účinnosti změny předpisů. V případě, že změna předpisů bude vydána až po datu účinnosti změny, tedy se zpětnou platností, sjednává se lhůta k nasazení do ostrého provozu nejpozději do 30 dnů od vydání příslušného právního předpisu ve sbírce zákonů.
6. Servisní garance – Dodavatel se zavazuje pro zajištění provozu IS garantovat zadavateli dostupnost služeb HelpDesk a Hot line v pracovní době dle konkretizace ve smlouvě.
7. Garance informovanosti – Dodavatel se zavazuje bez prodlení informovat zadavatele o veškerých softwarových produktech, nebo jejich částech, uvolňovaných v rámci této podpory a rovněž o všech nově samostatně dodávaných funkcích a modulech IS. Dodavatel se dále zavazuje bez prodlení informovat zadavatele o všech bezpečnostních incidentech a zranitelnostech dodávaného SW. Bude-li zajištění podpory provozu IS vyžadovat změnu či aktualizaci databázového prostředí, systémových softwarových či technických prostředků (dílčích komponent či celých zařízení), instalace a implementace upgradů nebo vyšších verzí databázových či systémových software nebo výměnu celých technologických částí, zavazuje se dodavatel, že o této skutečnosti bude zadavatele informovat v předstihu tak, aby byl zadavatel

schopen tuto změnu akceptovat a zajistit provedení změny sám nebo prostřednictvím dodavatele, příp. dalších třetích stran.

8. Garance součinnosti – Dodavatel se zavazuje poskytnout asistenci pro technické incidenty spojené s fungováním aplikace zahrnující jeho integrace s jinými aplikacemi. Dodavatel se zavazuje poskytnout zadavateli k řešení vynucených změn veškerou součinnost a potřebnou službu.

8.4 Systémová podpora

1. Garance provozu – dodavatel poskytne nutné prostředky ke zprovoznění celého řešení. Licence operačního systému a databází jsou součástí dodávaného řešení. Dodavatel bude mít serverovou část řešení (včetně databáze), operačního sytému a veškerých instalovaných aplikací kompletně pod správou. Dodavatel bude zajišťovat update operačního systému vždy na podporovanou verzi, která byla řádně otestována v testovacím prostředí. Jakékoliv zásahy do konfigurace přidělených HW prostředků bude dodavatel provádět pouze s koordinací se zadavatelem a naopak.
2. Garance bezpečnosti – Dodavatel se zavazuje po dobu platnosti této podpory řešit bezpečnostní chyby, hackerské útoky a zjištěné zranitelnosti.
3. Garance služeb migrace – Dodavatel se zavazuje po dobu platnosti této podpory zajistit pro zadavatele služby migrace – převod aplikace na vyšší verzi databázového prostředí a operačního systému. Dodavatel je povinen provést upgrade databázového prostředí a OS na vyšší verzi, pokud nebude původně instalovaná verze výrobcem SW v době trvání smlouvy již podporována. Instalační práce Dodavatele na převod – migraci jsou zahrnuty v paušální ceně Smlouvy.
4. Garance technické podpory výrobce – Dodavatel se zavazuje využít pro provoz DB prostředí zadavatele technickou podporu výrobce nebo Dodavatele databázového prostředí, které mu zprostředkuje zadavatel. Tato podpora zahrnuje zejména:
   - Přehled o SW opravách (patch) a vyžádání přístupu k těmto opravným kódům za účelem řešení chyb v programovém kódu příslušného produktu instalovaného u zadavatele.
   - Přístup do znalostní databáze „Knowledge database“ – aktualizovaná databáze technických referencí, která informuje o problémech, obsahuje vysvětlení chybových hlášení a další informace.
   - Přístup na Support Forum – možnost sdílení problémů a podpora řešení uživatelů databázových produktů.
   - Monitoring – Dodavatel je povinen po celou dobu účinnosti této Smlouvy zajišťovat monitoring v souladu s kapitolou Monitoring a dle Obchodních a platebních podmínek, bod 8.2.
   - Zálohování – Dodavatel je povinen po celou dobu účinnosti této Smlouvy zajišťovat zálohu IS v souladu s kapitolou Návrh a popis zálohování, obnovy a kontinuity navrhovaného řešení**.**

8.5 Služby podpory provozu

Uchazeč se zavazuje po dobu platnosti této podpory zajistit pro zadavatele následující služby spojené s podporou funkčnosti a provozu ASW:

Tabulka 2: Přehled profylaktických činnosti a jejich četnost

Přehled profylaktických činností	Četnost
Kontrola zálohování dat	1x měsíčně
Kontrola obnovitelnosti zálohy dat	1x za 6 měsíců

Tabulka 2: pokračování

Přehled profylaktických činností	Četnost
Kontrola konfigurace a nastavení ASW	Při update nebo upgrade ASW
Kontrola konfigurace a optimalizace DB prostředí	Při významné změně DB modelu nebo update DB systému, min. 1x ročně.
Kontrola aktuálnosti OS (zapracování kritických update)	1x měsíčně
Kontrola a analýza chybových či varovných logů ASW	1x za 2 týdny
Kontrola a analýza chybových či varovných logů DB	1x za 2 týdny
Kontrola performance logů	1x měsíčně
Kontrola systémových zdrojů	1x měsíčně
Provedení penetračních testů	Při upgrade ASW, DB, OS nebo integračních rozhraní
Provedení testu obnovy ze zálohy	1x ročně

1. Zadavatel požaduje 1x ročně vypracování zprávy, která bude obsahovat výstupy z profylaktických činností.
2. Zadavatel požaduje 2x ročně informaci o kontrole platnosti a aktuálnosti číselníků a upozornění na potřebu legislativního update.
3. Součástí profylaktických činností dle Tabulky 2 bude také kontrola bezpečnosti logů min. 1x měsíčně.
4. Zadavatel požaduje zprávy ukládat v Úložišti dokumentů.

8.6 Služby na vyžádání

Dodavatel se zavazuje po dobu platnosti této podpory zajistit pro zadavatele následující služby spojené s podporou ASW:

1. Konzultace a ostatní služby – konzultační služby jsou poskytované zpravidla v místě zadavatele dle sjednaných oblastí nebo pracovišť zadavatele. Konzultační služby mohou být po dohodě poskytnuty i vzdáleně. Z poskytnutých konzultací a ostatních služeb je vždy zápis. Konzultace a ostatní služby zahrnují:

- konzultační činnost pro uživatele a správce ASW,
- zaškolení uživatelů při rutinním provozu na pracovišti zadavatele,
- zaškolení správce ASW při implementaci nových verzí,
- metodická podpora při rutinním používání ASW,
- sledování využití ASW a vypracování návrhů na jeho zlepšení (proškolení uživatelů ASW, organizační opatření, posílení, doplnění nebo přesuny techniky apod.),
- metodická podpora konfigurace ASW a přípravy číselníků ASW,
- vytvoření databázového view na základě požadavku zadavatele.

Služba konzultační návštěvy bude realizována na základě dílčí objednávky a bude hrazena dle ceníku Služby na vyžádání (vysoutěžená hodinová sazba).

- Konzultační návštěvy jsou realizovány návštěvami pracovníků dodavatele na pracovišti zadavatele.
- Konzultace na dálku jsou poskytovány zejména prostřednictvím telefonu, online meetingů a dále elektronickou formou prostřednictvím záznamů HelpDesk, případně emailem.

- Jednotlivé konzultační návštěvy jsou zaměřeny vždy na konkrétní oblast. Maximální rozsah konzultační návštěvy je jeden člověkoden (tj. 8 hodin běžné pracovní doby). Do této doby je zahrnuta příprava dodavatele na provedení konzultační návštěvy, samotné provedení návštěvy a následné zpracování výsledků návštěvy formou protokolu.
- provedení konzultační návštěvy bude pracovníkem dodavatele vypracován protokol v elektronické podobě, který bude předán zadavateli.
- V Úložišti dokumentů je pro potřeby zadavatele současně uložen přehled čerpání konzultačních návštěv.

2. Realizace požadavků na novou funkcionalitu nad rámec poptávaného řešení – Služba programátorské a vývojové práce – služby poskytované zadavateli na základě dílčí objednávky, bude hrazena dle ceníku Služby na vyžádání (vysoutěžená hodinová sazba).

9. Akceptační kritéria dodaného řešení

Akceptační kritéria dodaného řešení vycházejí z tohoto dokumentu. Pro akceptaci je nutné splnit požadavky specifikované v předchozích bodech. Podrobně budou pro každou položku vyspecifikována v Předimplementační analýze. Tato kritéria budou posouzena objednatelem a případně doplněna o vlastní akceptační kritéria. U funkčních požadavků to znamená otestování všech evidencí a postupů zmíněných v kapitole 6 a pokud možno na všech předpokládaných platformách.

Dále pak provedení migrace dat, otestování provozu na různých požadovaných platformách, provedení stres-testů (simulovaný výpadek), předání nástrojů na správu jednotlivých aplikací, nástrojů na vyhodnocení logovaných událostí, nástrojů na správu uživatelských oprávnění, otestování jednotlivých API. Zároveň též předání dokumentace k uživatelským i správcovským částem systému, stejně tak jako k jednotlivým API, která jsou podle požadavků jeho součástí. Akceptační proces předmětu zakázky bude realizován následujícím způsobem:

- Bude vytvořena akceptační komise (členové projektového týmu, vedení FEL a CIV)
- Bude posouzena úplnost dodávky plně (dle smlouvy)
- Bude zpracován seznam připomínek a odevzdán dodavateli
- Dodavatel zapracuje připomínky
- Bude posouzeno zapracování připomínek

Závěr akceptační komise:

- Akceptováno
- Akceptováno s výhradami
- Neakceptováno

Pokud nebudou výstupy akceptovány, dojde k sankcím dle smlouvy.

10. Minimální technické podmínky

Pro účely zadávacího řízení jsou stanoveny minimální technické podmínky uvedené v kapitole 5.

11. Exit plán

Dodavatel předloží Exit plán, který bude minimálně obsahovat tyto údaje:

- harmonogram jednotlivých činností vedoucí k ukončení spolupráce,
- podrobný popis činností a procesů souvisejících s ukončením smlouvy,

- způsob migrace a zajištění bezpečnosti dat,
- osoby odpovědné za provedení celého procesu,
- analýzu rizik a návrh opatření k eliminaci rizik,
- způsob likvidace/archivace nepotřebných dat.