Příloha č. 1 – TECHNICKÉ PODMÍNKY

veřejné zakázky

s názvem

„Informační systém projektu CEITEC“

zpracované formou požadavků na funkci a výkon v souladu s ustanovením § 46 odst. 4 zákona č. 137/2006 Sb., o veřejných zakázkách (dále také jen zákon o VZ).

Obsah

1. POPIS ŘEŠENÉ PROBLEMATIKY

CEITEC – Středoevropský technologický institut je centrem vědecké excelence (dále jen „Centrum“) v oblasti věd o živé přírodě a pokročilých materiálů a technologií, jehož hlavním posláním je vybudování významného evropského centra vědy a vzdělanosti se špičkovým zázemím a podmínkami pro nejlepší vědecké pracovníky (viz http://www.ceitec.cz/onas/).

CEITEC vznikl ze společného projektu 6 nejvýznamnějších brněnských univerzit a výzkumných institucí za podpory Jihomoravského kraje a města Brna. Jeho nositeli jsou Masarykova univerzita, Vysoké učení technické v Brně, Mendelova univerzita v Brně, Veterinární a farmaceutická univerzita Brno, Výzkumný ústav veterinárního lékařství a Ústav fyziky materiálů AV ČR.

Základní stavební jednotku centra tvoří 64 výzkumných skupin s věcně nebo logicky souvisejícím výzkumným zaměřením, které jsou soustředěny do 7 synergicky spolupracujících výzkumných programů:

- Pokročilé nanotechnologie a mikrotechnologie,
- Pokročilé materiály,
- Strukturní biologie,
- Molekulární medicína,
- Molekulární veterinární medicína,
- Genomika a proteomika rostlinných systémů,
- Výzkum mozku a lidské mysli.

Zdrojem financování je Evropský fond pro regionální rozvoj, z něhož bude čerpat prostřednictvím Operačního programu Výzkum a vývoj pro inovace (dále jen „OP VaVpI“), prioritní osa č. 1 – Evropská centra excelence, který řídí MŠMT.

Požadovaný informační systém (dále také jako „IS“) má sloužit jako aplikační podpora primárních procesů Projektu a má zajistit plnou elektronizaci činností spojených s řízením dotačního managementu pro příjemce a partnery Projektu v plném souladu s legislativou a pravidly pro poskytování dotací z fondů EU. Systém má zefektivnit a plně zautomatizovat také proces reportingu projektu CEITEC vůči řídícímu orgánu, kterým je Ministerstva školství, mládeže a tělovýchovy České republiky (dále jen MŠMT).

Informační systém bude pokrývat činnosti spojené s řízením procesů dotačního managementu, plánování a další podpůrné procesy, které budou zahrnovat evidenci souvisejících projektů, nikoli vnitřní provoz svůj a partnerských institucí.

Základní oblasti, které budou řešené v rámci informačního systému:

- finanční management Projektu včetně reportingu, auditingu a controllingu
- evidenci dotačních výzev a k nim příslušných projektů, průběžný monitoring Projektu vzhledem ke všem navrženým indikátorům
- průběžný monitoring Projektu vzhledem k plnění harmonogramu

- řízení dokumentace k jednotlivým projektům včetně strukturovaného úložiště (DMS)
- komunikace s účastníky projektu a externími subjekty (CRM)
- prostředí pro komunikaci s pověřenými osobami žadatelů (mail, kalendář, portál web)
- nástroje pro plánování zdrojů (zaměstnanci, zařízení, finance, přístroje …)
- elektronická podpora agendy (plánování, kontrola, harmonogram …)

1.1. Procesy

Činnosti lze rozdělit z pohledu základních procesů na následující:

1.1.1. Dotační management

Administrace projektu vůči MŠMT dle pravidel OP VaVpI v souladu s aktuálními metodikami MŠMT a EU. Podrobný popis obsahuje PŘÍRUČKA PRO PŘÍJEMCE OPERAČNÍHO PROGRAMU VÝZKUM A VÝVOJ PRO INOVACE 2007 – 2013 včetně příslušných příloh (http://www.msmt.cz/strukturalni-fondy/prirucka-pro-prijemce-op-vavpi-2007-2013). Uvedená příručka obsahuje popis procesů, na základě kterých uchazeč navrhne metodiku workflow. Některé informace se vkládají přes informační systém BENEFIT7 (https://www.eu-zadost.cz/uvod.aspx), další informace jsou dosud evidovány v podpůrných evidencích aplikací MS Office (Excel, Word).

Dotační management je tvořen těmito činnostmi:

- zpracování průběžných zpráv o čerpání prostředků a stavu plnění projektu, tzv. monitorovacích zpráv (dále jen „MZ“) a žádostí o proplácení nákladů, tzv. žádostí o platbu
- evidence a kontrola dokumentace k veřejným zakázkám (dále jen „VZ“)
- monitorování řádného průběhu a vyhodnocení VZ dle platné metodiky a legislativy
- komunikace s účastníky projektu o průběhu projektu
- monitorování investiční činnosti pro potřeby projektu
- monitorování alokace pracovního času účastníků projektu na činnosti projektu
- monitorování strojního času pořízených zařízení pro potřeby projektu
- monitorování naplnění indikátorů projektu
- zpracování a evidence změnových řízení
- řízení rizik, řízení výjimečných situací
- správa projektové dokumentace
- zpracování závěrečné monitorovací zprávy projektu

Uvedené procesy jsou dosud realizovány formou shromažďování dat ve formátu MS Office (xls, doc). Tato data pořizují partneři CEITEC ručně, příp. ze svých IS formou exportu sestav dle požadavků uvedených v Příručce pro příjemce a souvisejících přílohách (http://www.msmt.cz/strukturalni-fondy/prirucka-pro-prijemce-op-vavpi-2007-2013). Z

podkladů dodaných partnery se dále vytvářejí celkové sumární výstupy za projekt jako celek.

1.1.2. Evidence projektů

V rámci Centra se shromažďují a evidují výzvy a již realizované projekty v oblastech pokrývajících tematické zaměření CEITECu. Projekty podané partnery CEITECu budou evidovány v předem dané struktuře s možnostmi připojení a evidence souvisejících dokumentů a s možností filtrování dle jednotlivých kritérií a vytváření sestav.

1.1.3. Podklady pro Základní řídící dokumenty projektu

Kvartální podklady od partnerů pro Plán činnosti projektu a pro Souhrnnou zprávu o činnosti Projektu. Stručná struktura workflow je obsažena v Příloze č. 1 – Návrh workflow – Struktura základních řídících dokumentů, kde je schéma workflow řídící dokumentace projektu.

1.2. Uživatelské skupiny

Zadavatelem zakázky je veřejná vysoká škola - akademický subjekt, který spolupracuje s dalšími 5 akademickými subjekty. Konkrétní cílovou skupinou jsou tedy:

- Pracovníci administrativy CEITEC – cca 70 uživatelů s přístupovými právy interního uživatele (přístup i k finančním datům daného partnera)
- Administrátor – max. 2 uživatelé pro správu systému
- Správci aplikací – max. 5 uživatelů pro správu dat a uživatelskou customizaci
- Zaměstnanci projektu CEITEC – řádově stovky uživatelů z akademického prostředí s obecnými přístupovými právy interního uživatele

Podkladem pro stanovení počtu potřebných licencí veškerých produktů potřebných k sestavení řešení je následně uvedený výhled nárůstu fyzických osob (headcount), který je pro organizaci závazný v uvedených letech.

Rok	2011	2012	2013	2014	2015
Management Projektu	82	80	87	89	86
Zaměstnanci Projektu	675	811	871	984	1024

Dle uvedeného výhledu růstu počtu uživatelů uchazeč navrhne model licencování a financování. Je nutné, aby průběh nárůstu uživatelů byl zohledněn v návrhu projektu a v návrhu jeho fází včetně harmonogramu implementace.

1.3. Organizační struktura CEITEC

1.3.1. Základní členění Centra z hlediska organizačního:

- CEITEC – Centrální řídící struktura Projektu (dále jen „CŘS“),
- CEITEC – organizační jednotka (dále jen „OJ“), tzn. středisko pro konkrétního partnera

1.3.2. Členění Centra z hlediska výzkumného:

- Výzkumný program
- Výzkumná skupina

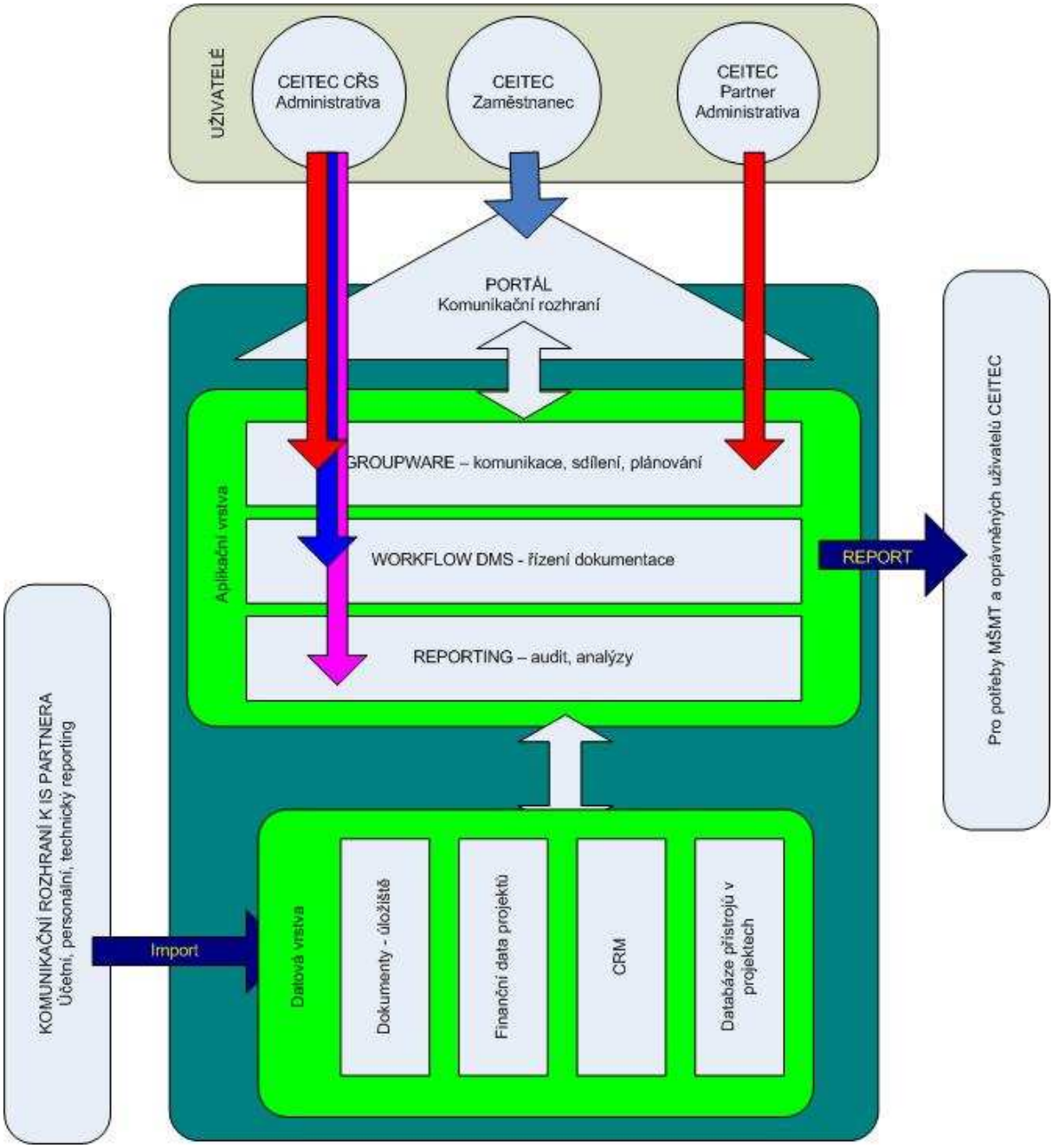
1.4. Popis prostředí:

Bezprostředním zadavatelem zakázky je samostatné hospodářské středisko CEITEC – CŘS, které je součástí Masarykovy univerzity (dále jen „MU“) a jako takové nevlastní počítačovou síť, nýbrž je součástí akademické sítě MU. Jde o specifickou organizační jednotku, která zajišťuje řídící, koordinační a administrační činnosti Projektu a nepokrývá žádné výzkumné a vývojové (dále jen „VaV“) aktivity. Výše uvedený fakt má za následek, že pracovníci CŘS mají pracovní stanice v adresném rozsahu MU a ostatní pracovníci organizačních jednotek u konkrétních partnerů – tj. v 6 různých sítích. Z uvedeného důvodu nelze uživatele CEITEC nijak oddělit pro účely provozu klasického interního IS v prostředí LAN. Kromě výše uvedeného většina uživatelů využívá i mobilní přístup z notebooku mimo pracoviště. Proto je nutno navrhnout řešení pro IS provozovaný vzdáleně, kde přístupovým médiem bude internet a klientem na pracovní stanici prohlížeč. Pro obecný uživatelský přístup dodavatel navrhne způsob zabezpečeného přístupu a dále přístup pro administrátory systému. Síťové prostředí partnerů, kde jsou umístěny pracoviště organizačních jednotek Centra (včetně CŘS), jsou chráněna na perimetru standardními prostředky (např. firewallem) a nepřipouští jakékoli výjimky v provozu, proto je nutno se omezit na běžně dostupné porty http a https a nelze pro přístup vnitřních uživatelů vyžadovat výjimky v nastavení perimetru partnerů CEITEC. Totéž platí pro sítě partnerů, kde nelze pro provoz tohoto systému měnit politiky a nastavení ochrany sítí.

2. OBECNÁ ARCHITEKTURA:

Na obrázku č. 1 je schematický zobrazena základní představa zadavatele o architektuře IS.

Obrázek č. 1



IS bude postaven v jednotném databázovém prostředí, základním stavebním prvkem bude SQL databáze, kde budou umístěna veškerá data včetně metadat.

IS bude obsahovat DMS pro řízení workflow a ukládání dokumentů. Funkcionality jsou uvedeny dále v textu tohoto dokumentu.

IS musí umožnit prostřednictvím Groupware (viz bod 3. 1.) všem uživatelům možnost zřídit účet pro komunikaci s Centrem (mail, instant messaging). Účet bude představovat prostředí, kde uživatel má k dispozici mailbox, kalendář a přístup k vybraným aplikacím či dokumentům Centra formou „pracovní desky“. K přístupu bude používat PC či notebook, obecně pracovní stanici v konfiguraci pro standardní přístup k internetu.

Výstupem z IS bude část (modul) reportingu, kde bude možno sestavit interní sestavy a reportovací sestavy dle metodických pravidel vypisovatelů výzev (primárně viz uvedená metodika MŠMT). Tyto reporty budou vázány na čerpání finančních zdrojů v oblasti investic (pořízení staveb a zařízení) a neinvestic (služby a ostatní provozně-personální výdaje).

Součástí bude podpora CRM, kde budou evidovány kontaktní informace o partnerech, zaměstnancích partnerů, zaměstnancích Centra, tj. o všech účastnících realizovaných projektů, včetně historie a vazeb na konkrétní projekty, a dále i o externích subjektech spolupracujících s Centrem. Konkrétní funkcionality naleznete v bodě 3.1.

Předpokladem uživatelského rozhraní je univerzální komunikační rozhraní pro všechny kategorie uživatelů formou PORTÁLU. Jejich kategorizace a segmentace bude provedena formou přístupových práv. Portál bude mít prvotní funkci informačního zdroje pro uživatele internetu. Prostřednictvím přihlášení získává uživatel přístup do své sekce, kde má možnost využívat aplikace GROUPWARE (mail, kalendář, dokumenty, kontakty a veškeré údaje o svých projektech).

IS bude obsahovat robustní a výkonný nástroj vyhledávání, který umožní nejen klasické, ale i kontextové hledání pro všechny typy uživatelů tak, aby časové zpracování bylo únosné a bylo možno rozlišit hledání v sekcích či v celém IS.

2.1. Obecné požadavky na hardware architekturu

Zadavatel předpokládá řešení formou hostování aplikace na hardwaru (dále jen „HW“), který bude v plné režii uchazeče. Součástí nabídky bude pouze návrh konfigurace HW, na kterém bude IS provozován tak, aby zadavatel měl informaci o poskytnutých kapacitách pro provoz IS, ukládání dat v IS, zálohování a možnostech přístupových kapacit.

Zadavatel požaduje v nabídce předložit návrh či popis zabezpečení IS před neoprávněným přístupem prostřednictvím internetu. Dále návrh či popis zabezpečení celého IS před neoprávněným přístupem k datům i samotné aplikaci a proti obecnému napadení.

Provoz IS bude chráněn proti škodlivému obsahu – Xware (antivir, antispam a další).

Aplikace budou chráněny před neoprávněným přístupem, neoprávněnou modifikací dat a dokumentů.

Uchazeč v nabídce uvede popis a přesnou adresu místa, kde bude IS hostován. Dále pak bude součástí popisu návrh či popis fyzického zabezpečení, zabezpečení proti výpadkům elektrické energie a proti živelným pohromám.

Popis musí obsahovat návrh DRP (disaster recovery plan) pro případ rozsáhlých výpadků a garanci záchrany a obnovy veškerých dat v IS. Zálohování systému musí umožnit v případě jakéhokoli výpadku 100% obnovu systému. Zadavatel předpokládá zálohování aplikací včetně nastavení a konfigurace a zálohování dat. Zálohy musí být dostatečně aktuální – záloha aplikace vždy při změně nastavení a záloha dat vždy za předchozí den (záloha aktuální 24 hod.).

2.2. Požadavky na autentizaci uživatelů

Zadavatel požaduje komunikační uživatelské rozhraní (klient) pouze prostřednictvím browseru (internetového prohlížeče), vyjma klientského rozhraní pro přístup administrátorů systému. Přístup bude zabezpečen prostřednictvím web aplikace, která bude využívat pro přístup uživatele více metod dvoufaktorové autentizace uživatelů včetně jejich kombinací:

- řešení musí splňovat podmínku všestranné autentizační platformy podporující různé služby (webové a ostatní)
- řešení musí podporovat autentizační protokol RADIUS
- autentifikátory musí podporovat standard OATH a algoritmus generování jednorázová hesla založený aspoň na 3 proměnných (jako čas, událost, soukromý klíč)
- uživatelé se autentizují pomocí hardwarových tokenů nebo softwarových tokenů
- softwarové tokeny musí být dostupné ve formě instalace na mobilní telefony, počítač s operačním systémem Windows a pomocí webového rozhraní (token na webu)
- řešení musí podporovat tyto autentizační metody: statické heslo, bezpečnostní otázky, one time passcode, out-of-band (pomocí sms zprávy nebo emailu), LDAP, PKI
- auditing: systém udržuje zabezpečený, a nemodifikovatelný log o autentizaci, administraci a o autorizačních požadavcích
- každý řádek v logu auditního systému musí být digitálně podepsán pomocí HSM modulu a obsahuje unikátní sekvenční identifikátor
- řešení musí disponovat API veřejným rozhraním, aby externí autorizovaný systém mohl také zapisovat do auditního logu
- data uložená v databázi, jako hesla, bezpečnostní otázky, PINy musí být šifrované pomocí HSM modulu
- všechna data v databázi jsou digitálně podepsaná
- zařízení má HSM (hardware security module) modul pro ochranu uživatelských dat (credentials) a privátních částí tokenů, dále slouží pro management klíčů a podepisování auditních informací

- řešení podporuje přístup pomocí API rozhraní klientům pro Javu, C++/#, C dostupných pomocí SOAP/RMI
- řešení má uživatelskou bázi v LDAP struktuře ActiveDirectory a zároveň je možné využít lokální databázi
- řešení musí umožňovat lokální inicializaci tokenů s určeným dedikovaným inicializačním nástrojem tak, aby privátní části byly známé jen organizaci (nikoliv třetí straně)
- řešení musí umožňovat použití tokenu, který je chráněn PINem zadávaným na klávesnici, ale také pomocí tokenu, u něhož se použije softwarový PIN (zadává se např. jako součást vstupního hesla)
- řešení musí disponovat rozšiřitelným rozhraním pro přidání autentizačních metod třetích stran v budoucnu
- řešení musí umožňovat přidání více autentizačních zařízení jednomu uživateli
- řešení musí umět management životního cyklu autentifikátorů jako je import, přiřazení, odlockování, synchronizaci
- řešení musí být ovladatelné pomocí webového rozhraní chráněného dvoufaktorovou autentizací
- řešení musí umožňovat kompletní oddělení dat pro různé skupiny uživatelů (např. interní uživatelé nebo externí partneři) v jedné instalaci tak, aby mohli být uživatelé v různých skupinách a jejich konfigurace a audit mohla být řízena pomocí různých operátorů
- řešení musí umožňovat řízení detailních práv skupin nebo uživatelů na základě rolí

3. POŽADAVKY NA FUNKCE INFORMAČNÍHO SYSTÉMU

IS by měl být složen z uvedených komponent tak, aby umožňoval tzv. úplnou integraci. Veškeré dále uvedené procesy bude možno provést plně elektronickou formou bez nutnosti použití jakéhokoli jiného přenosového médie včetně dalšího zadávání již v IS zadaných dat.

Zadavatel požaduje prostředí IS splňující maximální uživatelskou přívětivost a komfort ovládání. Uživatelské prostředí by mělo umožnit uživateli přizpůsobit „obrazovku“ svému etalonu (představě) pohodlného a přehledného ovládání (navrhněte, do jaké míry bude customizovatelné prostředí uživatele). Je vhodné navrhnout vybrané přístupy až na úroveň optimalizace pro zařízení typu PDA a SmartPhone.

Veškeré pracovní operace bude možno provádět prostřednictvím klienta v prohlížeči. Tzv. těžkého klienta typu klient-server lze použít pouze k administraci IS.

IS bude umožňovat navázání na produkty typu kancelářského balíku (textový editor, tabulkový procesor) pro použití v případě exportu či importu dat, tvorby sestav a analytických prací.

Zadavatel preferuje maximální míru standardizace při návrhu systému z důvodu dostupnosti podpory a servisu.

3.1. Základní funkcionality komponent IS:

3.1.1. Groupware

- Poskytnutí mail účtu s přístupem IMAP.
- Sledování a monitoring změn v systému včetně centrálního monitoringu a reportingu.
- Ochrana antispamovým řešením, které je napojeno na globální reputační systém kontrolující zdroj (IP adresu) a otisk samotné zprávy.
- Emailový klient – systém nabídne web rozhraní pro základní správu osobní pošty.
- Řešení je chráněno antivirovým řešením integrovaným přímo na logiku groupware a s napojením na globální heuristickou kontrolu.
- Poskytnutí kalendáře pro plánování událostí a možnost generovat pozvánky (propojení na CRM) či blokování zařízení (propojení na evidenci zařízení).
- Podpora kalendářů a jejich sdílení.
- Možnost standardní práce s adresáři kontaktů a selekce do skupin (hledání, filtrování).
- Možnost manuální údržby kontaktů či skupin – přidávání, odebírání, editace, tvorba vlastních číselníků.
- V ideálním případě i pravidelná, automatická aktualizace skupin podle definovaných kritérií (členové projektu, zaměstnanci pod vybraným partnerem, na určité pozici, roli, atd.).
- Zároveň je možné zobrazit seznam skupin, ve kterých je kontakt evidován.
- Práce s osobními složkami s možností přidělení práv k osobnímu adresáři.
- Možnost zasílání newsletterů (email s přílohou) – přednastavený formulář s rozesláním na všechny registrované kontakty (nebo skupiny) prostřednictvím emailu.
- Možnost práce s dokumenty, ukládání, generování a sdílení (omezený přístup, práva na data), např. personální agenda, dohody, smlouvy, pozvánky, komentáře.
- Řešení musí umožňovat sdílení tabulek z kancelářských aplikací na portálu, kde je bude možné upravovat pouze přes webové rozhraní.
- Portál musí umožňovat zobrazování dat (tabulek, grafů, reportů) uložených v aplikacích partnerů projektu.
- Podpora spolupráce přes diskusní fóra, chat.
- Optimalizace pro přístup mobilních zařízení.

3.1.2. DMS

- Podpora ukládání metadat k jednotlivým typům dokumentů.
- Na základě metadat systém umožní automatické vytváření souhrnu dokumentů od partnerů v definované (stromové) struktuře s možností předání do reportu.
- Uživatelské složky s předdefinovanou strukturou složek dokumentů, řízeno centrálně.
- Sledování a monitoring změn v řešení včetně centrálního monitoringu a reportingu bez vazby na oprávnění sledovaného řešení.
- Antivirová ochrana serveru, zajišťuje kontrolu spravovaných dokumentů v reálném čase i pomocí plánovaných skenů a je navázána přímo na logiku systému.
- Možnost přidělit oprávnění (čtení, zápis) - konkrétní roli na vybraný typ dokumentu.
- Možnost nastavení oprávnění na konkrétní dokument (bez volby typu dokumentu) pro vybraného uživatele.
- V rámci určité role (uživatele partnera) je třeba umožnit nastavení, kdy každý (autor) vidí pouze své dokumenty.
- Verzování dokumentů.
- Možnost práce se standardními formáty (minimálně txt, doc, xls, pdf, uveďte seznam formátů).
- Řešení umožní provádět automatizovanou kontrolu dat uložených v IS, která zajistí, že IS není zneužíván k ukládání soukromých nebo nevhodných dat. Musí být možné kontrolovat obsah minimálně následujících formátů dokumentů – txt, doc, xls, pdf.
- Možnost použití společných složek (Templates, další obecné složky).
- Možnost založit uživatelsky definované WF, např. Schválení dokumentu.
- Uložení řídících dokumentů (přístup pro všechny ke čtení, pro zápis jen CEITEC-CŘS), příručky, návody, společná pravidla.
- Možnost vytváření hierarchického systému dokumentů.
- Nástroj pro vyhledávání v dokumentech.
- Hledání v názvech.
- Hledání v dokumentech fulltext.
- Je třeba zajistit možnost načítání dat z vybraných typů souborů (více druhů XLS dokumentů – zejména účetní podklady) pro účely konsolidace dat za všechny partnery, výzkumné programy, výzkumné skupiny do stejného formátu výstupu.
- Vlastnictví definice struktury XLS není na straně CEITEC, ale MŠMT, tzn. struktura XLS dokumentů, jejichž data je nutné načítat do IS, se může měnit. Tomu je třeba přizpůsobit řešení, ideálně tak, aby při změně struktury XLS nebylo třeba zasahovat do kódu aplikace. Možnosti změn struktury XLS budou definované/závazné (např. neměnit Pojmenované oblasti apod.). Při změnách v

XLS je tedy nutné respektovat části struktury sloužící ke správnému načítání dat do systému.

- Evidence výběrových řízení (dokument v DMS) a připojených příloh.
- Řešení umožní vytváření workflow (dále jen „WF“).
- Podpora schvalovacího workflow, bude spouštěno pouze nad jednou (aktuální) verzí dokumentu.
- Je nutné zajistit průkaznost a autorizace dat. V rámci WF nad vybranými typy dokumentů je třeba mít možnost dokument zamknout před změnami.
- Příklad jednoduchého WF:
  - Partner uživatel - editace dokumentu (vypracoval).
  - Partner uživatel - schválení dokumentu (schválil), může i editovat.
  - Partner administrátor projektu – schválení dokumentu a „předání“ CŘS nebo hromadné schválení všech dokumentů za partnera a období a „předání“ CŘS.
  - CŘS administrátor projektu – akceptace nebo zamítnutí/vrácení podkladu.
- Je třeba uchovávat historii WF = evidence historie schvalování jednotlivých dokumentů.
- Řešení musí reportovat a případně blokovat soubory přesahující definovanou velikost.

3.1.3. Finanční data

- Umožní tvorbu standardizovaného rozhraní k ERP systémům partnerů pro možnost export/import reportovaných dat (např. SAP, Magion. iFIS apod).
- Vytváření reportů dle metodiky MŠMT (vytváření z ERP systémů partnerů i ručně).
- Vytváření sestav pro potřeby reportů (včetně ukládání šablon).
- Možnost plánování finančních toků a propojení na kalendář.
- Finanční data budou provázána na konkrétní projekty a osoby.
- Umožní pohled na historii formou provázání reportovaných dat (vývoj projektů v čase z finančního hlediska).
- Podpora Business Inteligence.
- Mzdové náklady – sledování, reporting nákladů vztahujících se k projektu (propojení na CRM)
- Při provedení importu dat z ERP partnerů bude nastavena kontrolní sestava a po její verifikaci pracovníkem CEITEC – OJ bude, povolen vlastní import do IS.
- Veškerá data k importu musí být možno editovat s možností uchování originální dávky.
- Import/export dat v režimu off-line, on-line, možnost automatického nastavení i ručního vyvolání tzv.“na tlačítko“.

- Tvorba rozhraní mezi ERP systémy partnerů a IS není součástí projektu, je věcí každého partnera. IS umožní podporu uvedené funkcionality.

3.1.4. CRM

- Sdílení kontaktů (obecně přístupné). Obsahem je zjednodušená evidence kontaktů - interních i externích subjektů. Evidované údaje jsou podobné jako u zaměstnanců, resp. eviduje se méně informací.
- Ukládání dokumentů a informací ke kontaktům (omezený přístup).
- Historie komunikace s kontaktem (omezený přístup).
- Využití strojů a přístrojů kontaktem (omezený přístup).
- Aktivity kontaktu/uživatele v systému.
- Zasílat Newslettery? Default = ANO (pouze privátní a administrátor)
- Souhlas se zpracováním osobních údajů? (pouze privátní a administrátor)
- Poznámka ke kontaktu: textové pole (administrátor)
- Evidence zaměstnanců a jejich úvazků, docházky, práce na projektech a úkolech
- Výstupem je standardní formát TS (XLS dokument), podpora schvalovacího WF
- Zaregistrování nového uživatele k IS (v případě nástupu nového zaměstnance). Evidenci uživatelů řeší admin CŘS (všichni uživatelé) nebo admin partnera (vidí a zakládá pouze uživatele/zaměstnance - partnera)
- Sledování a upozornění v případě změn osob ve vedoucích a seniorských pozicích – podstatná změna projektu
- Úkoly – nastavení úkolů, možnost přiřadit úkol k uživateli a WF úkolu, fáze úkolu, vyhodnocení úkolu
- Vybrané údaje zaměstnance jsou chráněny a zpřístupněny určité roli (vybraný pracovník partnera nebo centrály CŘS), kontaktní údaje přístupné všem
- Evidence pozic zaměstnanců v rámci jednotlivých projektů
- Automatické ukládání příchozích a odchozích emailů s automatickým zatříděním k odesílateli a příjemcům, ke společnostem, pro něž pracují odesílatel a příjemci
- Správa dostupnosti zdrojů (zasedací místnosti, stroje, osoby) včetně specifikace "pracovní doby" (aby nebylo možno rezervovat osobu například mimo její sjednanou pracovní dobu)
- Výkaz práce osoby
- Výkaz práce zdroje
- Možnost úpravy výkazů práce před jejich finálním odevzdáním
- Více možností tisku a odeslání elektronické verze výkazu práce (může sloužit i jako podklad pro výpočet mzdy)
- Dashboard se zobrazením individuálních výkonových cílů (například počet odpracovaných hodin, počet využití specifických zdrojů apod.)

- Přehledné zobrazení úkolů a upozornění na termíny, do kdy má být dokončen úkol
- Dohledatelnost aktivit typu email, schůzka, záznam z telefonátu, zápis z jednání u jednotlivých osob, institucí, firem, grantových žádostí
- Spolu s mailboxem možnost "odnést si práci s sebou a pracovat offline"
- Silná podpora WF, založená na možnosti práce napříč IS
- Tvorba průzkumů a dotazníků
- HelpDesk pro uživatele
- Znalostní Báze pro uživatele
- Správa konferencí (Evidence účastníků, správa konferenčních místností, registrace na jednotlivé přednášky, hodnocení, správa přednášejících a audiovizuální techniky)
- Diskusní fóra

3.1.5. Administrace systému

Je třeba rozlišit Administrátora IS od administrátora projektu. V této kapitole se zabýváme výhradně administrací IS. Zadavatel požaduje průběžnou informaci o stavu provozu IS a to na minimální úrovni uvedenou v následujícím textu kapitoly. Dále jsou zde uvedeny nároky na vlastní funkcionality IS z pohledu administrace.

Informační systém

- Reporting – přednastavené reporty podle požadavků administrátora (třeba definovat), možnost vytváření dalších reportů administrátorem, případně řešeno uživatelskou podporou
- Správa uživatelů, reset hesla
- Nastavení uživatelských práv, možnost zablokování účtu
- Role uživatele řídí:
  - přístup k typům dokumentů
  - přístup k údajům zaměstnance, kontaktu
  - přístup k funkcím systému, jeho modulům
- Hotline a jeho administrace
- Správa FAQ sekce (časté dotazy)
- Hromadná korespondence, Modul pro systémové zprávy
- Vstup do historie aktivit uživatelů – možnost konfigurace míry detailu logů, resp. typů aktivit, které se mají logovat
- Administrace kontaktů – možnost změnit informace o uživateli, jeho zařazení k Partnerovi
- Správa projektů a úkolů
- Správa a prohlížení timesheets

- Monitoring fungování IS – velikost databáze, výkon IS a jeho historie
- Posílání syst. zpráv, posílají se jen interně v IS. Byl by tam speciální archív systémových zpráv.
- Možnost monitorování přístupů uživatelů a zaznamenávání jejich aktivity

Správa bezpečnosti

- K dispozici je jedna centrální konzole, která generuje reporty ze všech nasazených bezpečnostních nástrojů (vyjma řešení produktů typu Appliance)
- Šablony pro reporty je možné definovat dodatečně a původní reporty musí být plně customizovatelné.
- Reporty je možné generovat minimálně ve formátech xls, pdf, csv a xml.
- Reporty je možné automaticky zasílat emailem nebo ukládat do sdílené složky.
- Centrální reportovací konzole musí být dostupná přes webové rozhraní.

Risk management

- K dispozici bude nástroj pro skenování zranitelností ve všech zahrnutých operačních systémech
- Je také možné skenovat zranitelnosti webových aplikací minimálně podle:
  - OWASP Top 10
  - CWE Top 25
- Nástroj pro skenování zranitelností bude pro nalezené zranitelnosti automaticky zakládat tikety pro udržení přehledu o jejich nápravě.
- Testy musí být označeny podle toho, zda jsou potenciálně nebezpečné pro infrastrukturu nebo ne. Celý sken lze provést pouze s testy, které infrastrukturu neohrozí.
- Zařízení musí podporovat definice standardů OVAL, XCCDF, SCAP

3.2. Uživatelské moduly

3.2.1. Pracovní deska

Základní pracovní prostředí v prohlížeči (optimalizováno viz níže). Zde uživatel vidí primární informace o komunikaci (zprávy, maily, úkoly), o projektech (dokončené, rozpracované, podané ke zpracování, připomínkované) a dokumenty (uložené, k připomínkám, změny, nové). Dále bude mít zobrazeny další moduly, do kterých bude mít povolen přístup v rámci definice své role k organizaci.

Typy a verze používaných prohlížečů:

- MS Windows IE v. 7 a 8
- Mozilla Firefox 3x
- Gogole Crome 4x

- Apple Safari 4x

3.2.2. Komunikace

Klient pro elektronickou komunikaci typu mail, news, instant messaging, propojení na adresáře Kontaktů, propojení na ostatní uživatelské moduly. Možnost tvorby vlastních složek a archivace komunikace.

3.2.3. Kontakty

Přístup k databázi kontaktů (CRM), možnost vkládání kontaktů a tvorby vlastních adresářů (skupin), možnost individuálního sdílení dle rozhodnutí uživatele, přístup ke konkrétním kontaktům a adresářům dle přidělených uživatelských práv.

3.2.4. Kalendář

Přístup k vlastnímu plánovacímu kalendáři, vlastní plánování, možnost udělení sdílení dle uvážení uživatele, přístup ke sdíleným kalendářům dle přidělených uživatelských práv, každý kalendář má svého správce, který rozhoduje kolize a odpovídá za správnost. Modul musí umožnit vzájemné zasílání pozvánek, kolizních alertů a reportů vytíženosti dle kalendáře. Jednotlivé události je možno vázat na konkrétní projekty, aby bylo možno sledovat alokaci času uživatelů versus projekty.

3.2.5. Dokumenty

Modul umožní vkládat, stahovat, prohlížet a sdílet dokumentaci vlastní a jinou dle přidělených uživatelských práv, umožní tvorbu a sdílení šablon. Zde je dostupná dokumentace k připomínkování, lze ji verzovat a zaznamenávat metadata. V rámci uživatelů IS nebude nutno přeposílat dokumenty, ale bude možno předat jen odkaz na uložený dokument a případně heslo přístupu k dokumentu či složce.

3.2.6. Projekty

V tomto modulu uživatelé mají sumarizované informace o konkrétních projektech, a to jak svých, tak i ostatních, které budou mít dostupné dle přidělených uživatelských práv. Budou zde dostupné informace o reálném stavu, čerpaných a volných prostředcích, míra čerpání a využití strojového času a personálních zdrojů. K projektu zde bude evidována veškerá dokumentace, kontakty, reporty, žádosti o platbu, monitorovací zprávy atd. Uživatelé Centra zde naopak budou vytvářet tyto údaje a sumarizovat ve vztahu k jednotkám uvedeným v kapitole 1.3.

3.2.7. Rozpočet a ekonomika

Uživatel partnera zde bude mít možnost sestavovat plán rozpočtu ke konkrétním projektům, mít k dispozici dostupná data o finančním stavu svých projektů a projektů dle přidělených uživatelských práv. Pracovníci administrativy CEITEC zde budou kontrolovat importovaná data z ekonomických systémů partnerů, budou je moci verifikovat a upravovat pro potřeby reportingu či porovnávat s plánem rozpočtu. Budou moci sestavovat finanční reporty (podklady pro monitorovací zprávy) jak k jednotlivým projektům či jejich skupinám, tak i ve vztahu k partnerům. Příkladový report obsahuje Příloha č. 1, kde je příklad reportu, sloužící jako podklad pro Základní řídící dokumenty projektu (viz kap. 1.1.). Veškerá data bude možno plánovat a kontrolovat ve vztahu k organizační struktuře v kapitole 1.3.

3.2.8. Personální data

Bude obsahovat údaje o čerpání nákladů na Projekt a další související projekty realizované v Centru ve vztahu k jednotlivým uživatelům, zaměstnancům a osobám, kteří se na konkrétních projektech podílejí. Uživatelé partnerů budou do této části vkládat data pro potřeby sumarizace a sestavení reportu pro monitorovací zprávy

projektů. Uživatelé Centra budou v tomto modulu tyto reporty a zprávy sestavovat. Do tohoto modulu bude možno provádět i automatizovaný import z aplikací partnerů.

3.2.9. Přístroje

Modul bude obsahovat seznam přístrojů (vybavení) vázaných k jednotlivým partnerům, OJ, výzkumným programům a výzkumným skupinám. Zde bude možno ze strany uživatelů partnerů plánovat a sledovat vytíženost přístrojů v rámci projektů. Uživatelé Centra v tomto modulu budou provádět sumarizaci a reporting a výstupem bude podklad pro vykázání v monitorovací zprávě. Modul umožní standardizovaný přístup jednak k přístroji jako takovému a také ke skupině přístrojů označených jako „služba“. Nastavení „služeb“ bude volitelné ze seznamu dostupných zařízení (zdrojů). Modul umožní tvorbu číselníků pro uvedení parametrů zařízení a pro „služby“ tvorbu šablon služeb. Časový plán bude umožňovat více možností použití tzv. minimální časové jednotky plánování a to na úrovni plánování a monitorování minut, hodin a dnů.

3.2.10. Veřejné zakázky

tento modul bude obsahovat konkrétní údaje o výběrových řízeních partnerů ve vztahu k Projektu. Uživatelé partnerů budou data vkládat jednak ručně – přímo, nebo bude možno provést automatický import z aplikace dle určeného rozhraní. Uživatelé Centra prostřednictvím tohoto modulu zadávají, kontrolují, vyhodnocují a reportují stav jednotlivých VZ. Zde budou dostupné informace o vazbě na Projekt, harmonogram, dokumentaci (kompletní) a dokumentaci o průběhu VZ. Umožní stanovení kontrolního mechanismu pomocí milníků pro splnění činností dle metodiky MŠMT včetně alertů – výstrah s časovým limitem pro plnění.

3.2.11. Reporting

Zde bude uživatel vytvářet podklady pro sestavení monitorovací zprávy k Projektu a to ve spolupráci s pověřenými pracovníky Centra. Dále bude možno na základě reportování provádět i audit Projektu (viz metodika MŠMT).

3.3. Ostatní požadavky:

Zadavatel požaduje, aby IS měl jednotné klientské rozhraní, ze kterého bude možno vstupovat do všech modulů formou záložek a tlačítek. Zadavatel nepřipouští instalaci klienta na stanici, vyjma administrátorských přístupů pro správu dat a samotného IS.

Klientské prostředí zadavatel požaduje v AJ a ČJ včetně volitelného přepínání. Znamená to popis a označení ovládacích prvků v uvedených jazykových mutacích.

Veškeré investice na konfiguraci HW systému tak, aby vyhovoval kapacitně požadavkům na provoz (konfigurace HW) **NEJSOU** předmětem této zakázky a uchazeč je povinen je uvést pro orientaci tzv. sizing HW a výhled jeho rozvoje tak, aby byl vyhovující v následujících 5 letech a to včetně kapacity připojení hostované aplikace k internetu. HW určený k provozu IS nabídne uchazeč formou služby hostování IS. Zadavatel předpokládá, že bude vlastníkem softwarových licencí, aplikací a dat v IS.

Další funkční požadavky, týkající se obecně portálu:

- Přehled webových částí
- Rozkladový strom

- Rozsáhlé indexování webu
- Rozšiřitelná vyhledávací platforma
- Řídicí panely
- Knihovna datových připojení
- Kontextové vyhledávání
- Miniatury a náhledy
- Podobné výsledky hledání, analytik …
- Pokročilé zpracování obsahu
- Profily řazení

3.3.1. Ochrana portálu

Webová aplikace bude obsahovat bezpečnostní prvky pro ochranu před zneužitím a případným útokem. Webový provoz bude kontrolován bezpečnostním modulem webového aplikačního firewallu (dále WAF).

Vyžadované funkční vlastnosti bezpečnostního modulu WAF:

- Modul WAF musí umožnit režim zapojení in-line, v případě potřeby musí být schopen být zapojen do módu out-of-bound
- Musí umožnit detekci bezpečnostních problémů na základě signatur (back-end např. Apache nebo IIS, ale i pro samotnou aplikační vrstvu např. detekci XSS, různé typy injection apod.)
- Musí obsahovat learning mode pro naučení chování aplikace, WAF se učí chování uživatelů
- Monitoruje session, strukturu webu – URL stránky, použité parametry, typy parametrů, délku parametrů atd.
- Chrání webovou aplikaci proti útokům v databázi OWASP top 10
- Obsahuje ochrany proti DOS útoku na lámání hesla nebo počet přístupů
- Umí detekovat únik citlivých informací z webové aplikace
- Provádí korelaci bezpečnostních událostí, které jdou na webovou aplikaci s těmi, co jdou z webové aplikace
- Detekuje chyby ve webové aplikaci na výstupu a místo toho nabídne uživateli jinou stránku (např. že se stala chyba apod.)
- Zabrání útoku zasláním reset spojení
- Modul WAF podporuje failover funkcionalitu
- Znázorňuje incidenty s datem a časem výskytu včetně kategorie závažnosti
- Musí zobrazovat přenesené toky dat v závislosti na čase
- Monitoruje dostupnost webové aplikace v čase (tj. monitoruje výpadky).

- Monitorování výkonnosti portálové aplikace a přidělování systémových prostředků za provozu
- Znázorňuje počet sessions webové aplikace a znázorňuje počet pomalých, rychlých a běžných session v čase
- Znázorňuje URL, na kterých stráví webový server nejvíce času
- Znázorňuje URL, které jsou nejvíce navštěvovány
- Znázorňuje URL, na kterých se vyskytuje nejvíce chyb při připojení

3.3.2. Antivirová ochrana systému

- Je prováděna antivirová ochrana v reálném čase (aktuálně zpracovávané soubory) s napojením na globální heuristickou kontrolu s možností nastavení stupně citlivosti (porovnání otisku a informací o souboru se stavem ve světě kvůli odhalení vznikajícího nebezpečí).
- Automatické plánování antivirových skenů celých disků nebo vybraných částí s možností definovat, v jaké hodiny a dny během týdne smí sken běžet. Musí být možné zaručit, že ve vybrané hodiny nebude prováděn žádný sken.
- Řídicí systém automaticky přerušuje a spouští antivirové skeny v závislosti na vytížení systému a úložiště, na kterém je sken prováděn – informace o vytížení jsou čteny přímo v reálném čase
- Antivirové řešení umožňuje automaticky blokovat síťová spojení na sdílené složky v případě, že se na ně útočící stroj pokouší šířit malware.
- Řešení umožňuje zablokovat sdílení souborů při případné masové infekci, aby nemohlo dále docházet k propagaci

3.3.3. Zabezpečení databáze

- Možnost definovat pravidla v závislosti na chování databáze. Spuštění pravidla má za následek upozornění administrátora nebo blokaci akce. Pravidla mohou být definována v závislosti na:
  - konkrétní tabulce
  - uživateli
  - množství dat – např. lze blokovat načtení velkého množství emailových adres
- Databáze je pravidelně skenována na bezpečnostní zranitelnosti a reporty jsou dodávány administrátorům IS. Součástí reportu musí být návrhy na řešení nalezených bezpečnostních problémů.
- Bude aplikován mechanismus na prevenci útoků na databáze, který bude schopen na základě signatur identifikovat a blokovat útoky. Ochrana na základě signatury bude účinná i v případě, že zatím neexistuje záplata od výrobce databáze (umožní tedy oddálit a plánovat nasazování záplat).
- Výpadek (včetně jeho totální selhání) bezpečnostního mechanismu postaveného nad databází nesmí ohrozit dostupnost a stabilitu. Uchazeč musí dodat popis funkcionality řešení (na jakém principu je kontrola prováděna).

3.3.4. Zabezpečení systému jako celku

- Data uložená v databázi, jako hesla, bezpečnostní otázky, PINy musí být šifrovaná
- Lze spustit pouze kód, který je zahrnut v databázi povoleného softwaru pro daný systém (tzv. softwarový whitelist)
- Whitelist je vytvořen automaticky indexací
- Softwarové vybavení stroje (a s tím související whitelist) smí být modifikováno pouze vybraným softwarem definovaným jednou z následujících metod (jiný software nesmí modifikovat softwarové vybavení):
  - hashem – kontrolní součet spustitelného souboru (min.SHA1)
  - veřejným klíčem – spustitelný soubor je elektronicky podepsaný
  - umístěním – v lokální nebo síťové složce
  - pro jednotlivé aplikace se přesně vymezí možnosti síťového provozu (firewalling – podle portu, IP adresy nebo sítě, času) a aplikace se definují:
  - veřejným klíčem – za předpokladu, že spustitelný soubor je elektronicky podepsaný
  - umístěním a názvem – na souborovém systému
- Firewallová pravidla jsou centrálně definovatelná s využitím připravených šablon pro jednotlivé komunikace i aplikace
- Pokus o spuštění softwaru nezahrnutého ve whitelistu je zaznamenán a reportován do centrální konzole, samotné spuštění je zablokováno.
- Whitelisty mezi jednotlivými stroji bude možno porovnávat automaticky
- Ochrana whitelistem se vztahuje i na software, který je vykonáván interpretem (skripty) nebo virtuálním strojem (např. Java). Není tedy možné spustit skript, který není na whitelistu.
- Sledování a monitoring změn v systému včetně centrálního monitoringu a reportingu bez vazby na oprávnění sledovaného systému.
- Vybrané součásti aplikací a operačního systému lze chránit proti čtení a zápisu jiným mechanismem, než jsou standardní oprávnění operačního systému.
- Možnost tvorby libovolných pravidel pro generování upozornění na změnu systému poskládaných z následujících podmínek:
  - Soubor
  - Program
  - Registry
  - Uživatel
- Operační systém je chráněn IPS softwarem umístěným přímo na serveru a kontroluje síťovou komunikaci i systémové volání. IPS signatury jsou pravidelně aktualizovány s centrálně definovatelnou závažností a reakcí či možností centrálně definovat konkrétní pravidla na základě minimálně následujících atributů:

- Soubor
- Registry
- Program
- Služba
- Navázání DLL knihovny
- SQL dotaz
- HTTP požadavek

- Seznam aktualizovaných IPS signatur je k dispozici i s jejich popisem, resp. odkazem na zranitelnost, kterou pokrývají

4. IMPLEMENTACE

Návrh implementace bude zpracován v následující struktuře:

- Popis použité metodiky
- Návrh metodiky řízení projektu
- Rámcový návrh fází projektu včetně jejich detailního popisu (vstupy, výstupy, časová náročnost, nároky na součinnost)
- Detailní popis procesů testování a akceptace pro konkrétní fáze projektu
- Návrh rámcového harmonogramu (formou „slepého kalendáře“ T+x)
- Návrh kontrolních mechanismů a procesů včetně ukotvení v harmonogramu
- Změnová řízení – podrobná definice
- Návrh struktury a procesů schvalování projektové dokumentace
- Popis úrovně zapojení zadavatele do procesů implementace a zdůvodnění
- Návrh projektového týmu uchazeče včetně profesních CV členů týmu a role v týmu – musí odpovídat osobám, jimiž dodavatel prokazuje kvalifikaci.
- Vzory dokumentace
- Termín dokončení implementace nejpozději 7 kalendářních měsíců od uzavření smlouvy

Návrh bude obsahovat zejména:

- Popis procesu vypracování cílových konceptů, definice obsahu cílových konceptů (funkční model, datový model, data, role, vazby …) včetně schvalovacích procesů
- Fáze projektu musí být úplné a pokrýt všechny činnosti po dobu trvání projektu
- Každá fáze by měla obsahovat kontrolní mechanismy a procesy
- Harmonogram musí zohlednit prostor pro testování, ověřování a kontrolní mechanismy a musí být reálný

- Pro složení projektového týmu je nutné uvést požadovanou kvalifikaci pro zástupce zadavatele
- Metodika a navrhovaný rozsah školení s rozčleněním dle uživatelů
- Rozsah podpory pro fáze uvedení do ověřovacího a ostrého provozu

5. ÚDRŽBA, PODPORA A SERVIS SYSTÉMU

Uchazeč navrhne a popíše v jím zvoleném detailu, systém poskytování údržby IS a poskytování uživatelské podpory, včetně servisních podmínek.

Zadavatel vyžaduje v rámci těchto činností následující:

- Poskytování údržby, podpory a servisu po dobu pěti let
- Možnost nahlášení incidentu v režimu 7x24 (web, mail, telefon)
- Příjem hlášení o incidentech bude v režimu 5x10 (8-18hod v pracovní dny)
- Maximální reakční doba incidentu bude 2hod od nahlášení
- Zahájení řešení max. 6hod od nahlášení incidentu
- Odstranění závady max. 12hod od zahájení řešení incidentu
- Zajištění osobní přítomnost člena implementačního týmu (technického specialistu) 1x týdne na 2 hodiny v prostorách zadavatele
- Kompletní reporting o vzniku, průběhu a uzavření incidentu
- Záruční doba systému po celou dobu trvání kontraktu (5 let) včetně podmínek
- Aktualizace IS vzhledem k verzím softwaru
- Pravidelné reportování o provozu IS (včetně výkazu o bezpečnostních incidentech), oaktualizacích, patch managementu, nových verzích atd.
- Možnost monitorování přístupů uživatelů a zaznamenávání jejich aktivity
- Výrazně oddělit činnosti v rámci služeb placené podpory, údržby a servisu
- Výrazně oddělit pozáruční servisní podmínky

6. PŘÍLOHA

Příloha: Návrh workflow – Struktura základních řídících dokumentů

Návrh workflow –Struktura základních řídících dokumentů

1. Plán činnosti Projektu

Aktivita	Zpracovává	Schvaluje/ oponuje	Orgán/funkce
Plán činnosti Projektu	**Výkonný ředitel**	**schvaluje**	**Koordinační rada**
Plán vědecké činnosti Projektu včetně střednědobého a dlouhodobého výhledu	Vědecký ředitel	oponuje schvaluje	Mezinárodní vědecká rada Výkonný ředitel
Návrh rozsahu a kritérií Společného hodnocení vědecké excelence	Vědecký ředitel	schvaluje	Mezinárodní vědecká rada
Plán plnění společných výzkumných cílů	Vědecký ředitel	oponuje	Mezinárodní vědecká rada
Plán vědecké činnosti Výzkumného programu	Koordinátor Výzkumného programu	schvaluje	Vědecký ředitel
Plán vědecké činnosti Výzkumné skupiny	Vedoucí výzkumné skupiny	schvaluje / oponuje	Ředitel organizační jednotky / Koordinátor Výzkumného programu
Plán investiční činnosti	Operační ředitel	oponuje	Výkonný ředitel
Plán výstavby Partnera	Pověřená osoba Partnera	oponuje	Operační ředitel
Plán pořízení zařízení Organizační jednotky	Ředitel organizační jednotky	oponuje	Operační ředitel
Plán dalších činností Projektu	Operační ředitel	oponuje	Výkonný ředitel
Plán veřejných zakázek	Operační ředitel	schvaluje	Výkonný ředitel
Plán veřejných zakázek Organizační jednotky	Ředitel organizační jednotky	oponuje	Operační ředitel
Plán monitorování Projektu	Operační ředitel	oponuje	Výkonný ředitel
Plán monitorování Organizační jednotky	Ředitel organizační jednotky	oponuje	Operační ředitel

Plán dalších činností Organizační jednotky	Ředitel organizační jednotky	oponuje	Operační ředitel
Plán servisních činností Centrální řídící struktury	Operační ředitel	schvaluje	Výkonný ředitel
Plán hospodaření Projektu (konsolidovaný rozpočet)	Operační ředitel	schvaluje	Výkonný ředitel
Plán hospodaření (rozpočet) Centrální řídící struktury	Operační ředitel	schvaluje	Výkonný ředitel
Plán hospodaření (rozpočet) Organizační jednotky	Ředitel Organizační jednotky	oponuje	Operační ředitel

2. Souhrnná zpráva o činnosti Projektu

Aktivita	Zpracovává	Schvaluje/ oponuje	Orgán/funkce
Souhrnná zpráva o činnosti Projektu	**Výkonný ředitel**	**schvaluje**	**Koordinační rada**
Zpráva o plnění Plánu vědecké činnosti Projektu	Vědecký ředitel	schvaluje	Mezinárodní vědecká rada
Výsledky Společného hodnocení vědecké excelence	Vědecký ředitel	schvaluje	Mezinárodní vědecká rada
Zpráva o plnění společných výzkumných cílů	Vědecký ředitel	schvaluje	Mezinárodní vědecká rada
Zpráva o plnění Plánu vědecké činnosti Výzkumného programu	Koordinátor Výzkumného programu	schvaluje	Vědecký ředitel
Zpráva o plnění Plánu vědecké činnosti Výzkumné skupiny	Vedoucí výzkumné skupiny	schvaluje / oponuje	Ředitel organizační jednotky / Koordinátor Výzkumného programu
Zpráva o plnění Plánu investiční činnosti	Operační ředitel	oponuje	Výkonný ředitel
Zpráva o plnění Plánu výstavby Partnera	Pověřená osoba Partnera	oponuje	Operační ředitel
Zprávy o plnění Plánu pořízení zařízení Organizační jednotky	Ředitel organizační jednotky	oponuje	Operační ředitel
Zpráva o plnění dalších činností Projektu	Operační ředitel	oponuje	Výkonný ředitel
Zpráva o plnění Plánu veřejných zakázek	Operační ředitel	schvaluje	Výkonný ředitel
Zpráva o plnění Plánu veřejných zakázek Organizační jednotky	Ředitel organizační jednotky	oponuje	Operační ředitel
Zpráva o plnění společných pravidel Projektu	Operační ředitel	schvaluje	Výkonný ředitel
Zpráva o plnění společných pravidel Projektu Organizační jednotkou	Ředitel organizační jednotky	oponuje	Operační ředitel
Zpráva o dalších činnostech Organizační jednotky	Ředitel organizační jednotky	oponuje	Operační ředitel
Zpráva o plnění Plánu servisních činností Centrální řídící struktury	Operační ředitel	schvaluje	Výkonný ředitel

Zpráva o hospodaření Projektu	Operační ředitel	schvaluje	Výkonný ředitel
Zpráva o hospodaření Centrální řídící struktury	Operační ředitel	schvaluje	Výkonný ředitel
Zpráva o hospodaření Organizační jednotky	Ředitel organizační jednotky	oponuje	Operační ředitel