Příloha A-III

**SPECIFICKÉ POŽADAVKY NA SPOLEČNÉ DATOVÉ PROSTŘEDÍ (CDE)**

**Modernizace mostu ev.č.3227-3 Řečany nad Labem**

**verze ke dni zahájení řízení**

Obsah

[1 Úvod 3](#_Toc169187193)

[2 API CDE Objednatele 3](#_Toc169187194)

[3 Systémové požadavky 3](#_Toc169187195)

[4 Funkční požadavky 3](#_Toc169187196)

[5 Adresářová struktura 4](#_Toc169187197)

[6 Bezpečnostní požadavky 4](#_Toc169187198)

[7 Další požadavky 5](#_Toc169187199)

*Tento dokument byl zpracován s přihlédnutím k dokumentům vydaným Českou agenturou pro standardizaci v rámci Koncepce BIM, k SFDI Standardům a je v souladu s řadou norem ČSN EN ISO 19650:1-4.*

*Proconom Software, s.r.o.*

1. Úvod
   * 1. **Objednatel má vlastní CDE, v němž provozuje projekty.** Je upřednostňováno, aby si Dodavatel zajistil přístup do Objednatele používané aplikace, viz Příloha A [BIM Protokol], kapitola 2.2.1.
     2. V tomto dokumentu jsou uvedeny požadavky Objednatele na Společné datové prostředí (dále jen „CDE“), které vchází v platnost v případě, že si Dodavatel zajistí své vlastní CDE.
     3. Dodavatel zajistí kompatibilitu mezi použitím CDE Dodavatele a CDE Objednatele. Tato kompatibilita může být zajištěna prostřednictvím otevřeného API. Dodavatelem zvolené CDE bude splňovat požadavky uvedené v tomto dokumentu.
     4. Dodavatel zajistí přístup osob Dodavatele do systému CDE a použití systému CDE dle BIM Protokolu a jeho příloh.
2. API CDE Objednatele
   * 1. API CDE Objednatele je k dispozici na webové adrese: <https://suspceapi.digitalita.cz/swagger/index.html>
3. Systémové požadavky
   * 1. Dodavatel CDE zajistí technickou podporu (telefonicky/emailem) pro Objednatele   
        v pracovní dny od 9:00 do 16:00 hodin.
     2. Dodavatel zajistí nepřetržité propojení systémů skrze API na své náklady. V případě nefunkčnosti/nedostupnosti propojení, garantuje Dodavatel jeho opětovné zprovoznění do 72 h od telefonického/e-mailového nahlášení nefunkčnosti/nedostupnosti systému Objednatelem.
     3. Musí být použity takové technologie/principy, které zajistí požadovanou úroveň důvěrnosti, dostupnosti a integrity uchovávaných dat a informací.
4. Funkční požadavky
   * 1. Požadavky na jednotlivé funkce CDE:
        1. Stažení souborů a složek na úložiště mimo CDE.
        2. Revize souborů a složek.
        3. Integrované prohlížení souborů (formáty .pdf, .doc, .ifc, .xlsx a dalších běžně užívané formáty) a prohlížení nativních formátů BIM softwarů.
        4. Integrované prohlížení Digitálního informačního modelu stavby (DiMS).
        5. Systém CDE nesmí být omezen jen na určité formáty, ale musí umožňovat uložit jakýkoli relevantní formát souboru dokumentu v digitální podobě.
        6. Správa jednotlivých verzí souborů, jejich přístupnost v rámci systému.
        7. Tvorba vlastních pracovních postupů souvisejících se soubory.
        8. Notifikace na soubory.
        9. Vyhledávání v datech, full-text u dokumentu ve formátu .doc, .xls a .pdf.
        10. Filtrování, vhodná zobrazení dat v rámci aplikace filtru.
        11. Audity souborů.
        12. Správa uživatelských rolí a oprávnění uživatelů s různými úrovněmi přístupových oprávnění k celému BIM projektu a jeho jednotlivým složkám a podsložkám.
        13. Definice a správa defaultních pracovních postupů (podpora pracovních postupů – workflow).
        14. Vytváření úkolů přímo spojených s určitými místy v dokumentu (2D výkres / IFC model), jejich přiřazení konkrétním řešitelům, notifikace úkolů e-mailem.
        15. Přístup externím uživatelům do vyhrazeného prostoru a k vyhrazeným složkám, popř. souborům.
        16. Po ukončení provozu systém umožňuje export dat do adresářové struktury včetně logů, auditů a metadat.
5. Adresářová struktura
   * 1. Adresářová struktura bude předána Objednatelem na základě vyžádání BIM koordinátora Dodavatele do 10 dní od jejího vyžádání. Adresářovou strukturu je povinen Dodavatel dodržovat.
6. Bezpečnostní požadavky
   * 1. Systém zaznamenává auditní logy a umožňuje zástupcům Objednatele přístup k těmto informacím, které musí zahrnovat všechny informace o úpravách všech uložených souborů  
         a jejich metadat včetně informace, kdo se souborem manipuloval.
     2. Systém zaznamenává logy obsahující přihlašování/odhlašování uživatelů a umožňuje zástupcům Objednatele přístup k těmto informacím, které musí zahrnovat zejména časové razítko, přihlašovací jméno a popis události.
     3. Systém zaznamenává logy řešení pro ochranu před škodlivým kódem, v případě webové aplikace také logy řešení pro ochranu webových aplikací.
     4. Systém podporuje a vynucuje přístup přes šifrované spojení prostřednictvím webového prohlížeče (HTTPS) pro přístup k veškerým uloženým informacím. Použitý certifikát pro tento účel musí být podepsán důvěryhodnou kořenovou certifikační autoritou.
     5. Pokud Dodavatel Cloud Computingu (služby), který poskytuje tuto službu v České republice, nemá sídlo v Evropské unii a neustavil si svého zástupce v jiném členském státě Evropské unie, musí mít ustanoveného svého zástupce v České republice. Zástupcem Dodavatele Cloud Computingu je osoba, která má sídlo v České republice a která je Dodavatelem Cloud Computingu na základě plné moci zmocněná jej zastupovat.
     6. Dodavatel služby musí zajistit na základě žádosti Objednatele bez zbytečného odkladu přístup k informacím a datům, které Dodavatel služby uchovává, včetně možnosti kontroly uchovávaných informací a dat v reálném čase.
     7. Dodavatel služby musí zajistit řízení kontinuity činností v souvislosti s poskytovanou službou.
     8. V případě vyžádání Objednatele podepíše Dodavatel dohodu o mlčenlivosti (NDA) týkající se prací na projektu.
     9. Po skončení projektu budou data předána Objednateli na datovém médiu (CD, DVD, případně jiném dle dohody…), na kterém bude systém archivován včetně data a jejich atributů.
     10. Objednatel služby požaduje, aby Dodavatel služby informoval a bezpečnostních událostech, které mohou mít vliv na integrity, důvěryhodnost a dostupnost uchovávaných dat a informací.
     11. Dodavatel služby musí zajistit ochranu před škodlivým kódem nad Dodavatelem služby uchovávanými daty a informacemi.
     12. Dodavatel služby musí zajistit ochranu webových portálů proti průnikům nasazením vhodné web aplikační ochrany (např. web aplikační firewall).
     13. Řešení jako celek (všechny komponenty - OS, aplikace) musí být udržovány aktualizované a v případě zjištění specifické zranitelnosti aplikace musí být tato bezodkladně opravena.
     14. Z pohledu důvěrnosti se s informací může seznámit pouze jakýkoliv zaměstnanec Objednatele, nebo jejich konzultanti a pověřené osoby, nebo osoby Dodavatele. Ostatní osoby musí být schváleny Objednatelem.
7. Další požadavky
   * 1. Dodavatel bude v rámci společného datového prostředí udržovat aktuální dokumenty, digitální informační modely, průzkumy, výkresy, vyjádření, dokumentace dle Smlouvy o dílo tak, aby byly k dispozici Objednateli.
     2. Uživatelské rozhraní systému je v českém jazyce.
     3. CDE systém zohledňuje následující právní předpisy:
        1. zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů;
        2. vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby;
        3. VMV čá. 57/2017 Národní standard pro elektronické systémy spisové služby;
        4. zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů;
        5. vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů;
        6. zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů;
        7. vyhláška č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce   
           a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy);
        8. zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce;
        9. zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti);
        10. vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti);
        11. Nařízení Evropského parlamentu a rady (EU) 2016/679, obecné nařízení o ochraně osobních údajů (např. dodržením ISO 27001).