PŘÍLOHA A-I

POŽADAVKY NA CDE

verze ke dni zahájení řízení

OBSAH

ÚVOD[1]

Tento dokument vznikl na podkladu a v souladu s metodikami vydanými Českou agenturou pro standardizaci a Státním fondem dopravní infrastruktury.

Jako podklad pro tento dokument byla využita Metodika pro výběr společného datového prostředí (CDE), Státní fond dopravní infrastruktury, září 2019 a Příloha č. 2 BIM Protokolu, Požadavky na Společné datové prostředí, zpracovaná týmem PS02 a PS03 pod vedením Josefa Žáka a Lukáše Klee a vydaná Českou agenturou pro standardizaci 2021.

CDE je centrálním zdrojem informací používaným k jejich shromažďování, správě a sdílení pro celý projektový tým. Vytvoření tohoto centrálního zdroje informací usnadňuje spolupráci mezi jednotlivými účastníky Projektu, jednoznačně určuje platnou verzi informace a pomáhá vyhnout se nedorozumění, duplicitám a chybám.

Úlohou CDE tedy je řídit a spravovat dokumenty, procesy a komunikaci o Projektu ve fázích přípravy a provádění stavby a musí být použity takové technologie a principy, které zajistí požadovanou úroveň důvěrnosti, dostupnosti a integrity uchovávaných dat a informací.

1 SYSTÉM CDE A FUNKČNÍ POŽADAVKY

1.1 SYSTÉM CDE

CDE musí být integrovaný jednotný systém splňující následující požadavky.

CDE musí spojovat všechny požadované funkce CDE do jednotného prostředí ovládaného přes jednotné rozhraní.

Dodavatel musí v rámci CDE udržovat aktuální dokumenty, digitální modely stavby, průzkumy, výkresy, vyjádření, dokumentace a další dokumenty podle Smlouvy tak, aby byly k dispozici Objednateli.

1.2 FUNKČNÍ POŽADAVKY

CDE jako sdílené úložiště dokumentů v digitální podobě umožňuje manipulaci s těmito dokumenty pro potřeby všech procesů, tj. zejména:

- stažení souborů a složek na úložiště mimo CDE;
- revize souborů včetně jejich správy a případně revize celých složek;
- porovnání stejných dokumentů v digitální podobně s jejich předchozími verzemi;
- integrované prohlížení souborů s příponami (.pdf, .txt, docx., xlsx., jpg., png.);
- práce s dokumenty bez ohledu na jejich formát nebo příponu;
- sdílení a prohlížení fotografií;
- správa jednotlivých verzí (revizí) dokumentů, jejich přístupnost v rámci systému;
- audity dokumentů (např. formou audit logů) a dohodnutých procesů;

[1] V tomto dokumentu jsou používány definice uvedené v ust. 1.1 [Definice] BIM protokolu, jehož součástí je tento dokument. Pojem „**Projekt**" je projekt, v jehož rámci je prováděno Dílo ve smyslu Smluvních podmínek, které jsou součástí Smlouvy.

- vyhledávání v datech, včetně full-textového vyhledávání;
- filtrování, vhodná zobrazení dat v rámci aplikace filtru;
- workflow řešící předávání, schvalování apod. dokumentů, změnových řízení, popis způsobu vypořádání připomínek;
- definice a správa defaultních pracovních postupů (podpora pracovních postupů - workflow);
- práce s číselníky;
- nastavení oprávnění dle požadavků Objednatele;
- přístup externím uživatelům do vyhrazeného prostoru a k vyhrazeným složkám;
- po ukončení provozu CDE umožňuje export dat do adresářové struktury včetně logů, auditů a metadat.

1.3 LOGICKÉ VAZBY

Objednatel požaduje, aby CDE umožnovalo vytvoření odkazů na cesty (např. adresářové cesty, URL, hypertextový odkaz, …) směřujících na vybrané dokumenty v digitální podobě.

1.4 DATOVÉ FORMÁTY

Systém CDE nesmí být omezen jen na určité formáty a musí umožňovat uložit jakýkoli vhodný, resp. relevantní formát souboru dokumentu v digitální podobě.

1.5 JAZYKOVÉ MUTACE CDE

Uživatelské rozhraní CDE musí být v češtině.

1.6 TECHNICKÉ NORMY, PŘEDPISY A METODIKY

CDE musí zohledňovat následující předpisy v jejich aktuálních zněních:

- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti);
- zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů;
- vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby;
- VMV čá. 57/2017 Národní standard pro elektronické systémy spisové služby;
- zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů;
- vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů;
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů;
- 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);
- zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce;

- 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);
- Nařízení Evropského parlamentu a rady (EU) 2016/679, obecné nařízení o ochraně osobních údajů (např. dodržením ISO 27001).

2 ZPŮSOB LICENCOVÁNÍ, PRAVIDLA PRO PŘIDĚLOVÁNÍ LICENCÍ

2.1 LICENČNÍ PODMÍNKY

Náklady na CDE (licence) na straně Dodavatele jsou zahrnuty v Přijaté smluvní částce ve smyslu Smluvních podmínek, které jsou součástí Smlouvy.

Dodavatel musí umožnit přístup osob určených Objednatelem do CDE a použití CDE dle BIM protokolu, jehož součástí je tento dokument.

Dodavatel musí zajistit dostatečný počet licencí pro celý Projekt. Je na Dodavateli, zda dodá vlastní systém, tyto licence bude pořizovat jako uživatelské (licence na uživatele), nebo dle velikosti a trvání Projektu.

3 PŘÍSTUP A DOSTUPNOST

3.1 TECHNICKÉ ŘEŠENÍ PŘÍSTUPU

Dodavatel musí do pracovních 10 dní od zprovoznění CDE předat Objednateli popis API, aby CDE umožňovalo propojení se systémy ostatních pověřených stran. API bude specifikované minimálně do takového detailu, že umožní volání funkcí zajišťující požadavky v tomto dokumentu.

3.2 GARANCE DOSTUPNOSTI

Dodavatel musí zajistit nepřetržitou dostupnost, provozuschopnost a údržbu CDE. V případě nefunkčnosti/nedostupnosti CDE (mimo sjednaná plánovaná servisní okna) garantuje Dodavatel jeho opětovné zprovoznění do 8 hodin od telefonického/e-mailového/ nahlášení nefunkčnosti/nedostupnosti CDE Objednatelem nebo jakoukoliv třetí osobou pověřenou Objednatelem. Celkově Dodavatel garantuje provoz CDE (poskytne klientovi odezvu) minimálně 99 % času po dobu trvání Smlouvy mimo servisní okna.

Dodavatel musí na žádost Objednatele podrobně specifikovat způsob řešení nezbytných technických zásahů do CDE, které mohou vést k výpadkům funkčnosti, způsob řešení technických závad a minimalizace jejich dopadů na CDE. Dodavatel garantuje dostupnost CDE po dobu trvání Smlouvy.

V CDE musí být použity takové technologie/principy, které zajistí požadovanou úroveň důvěrnosti, dostupnosti a integrity uchovávaných dat a informací.

3.3 GARANCE EXPORTU DAT

Dodavatel musí na vyzvání Objednatele do 10 pracovní dní deklarovat bezpečnost uložených dat, jejich dostupnost a zajistit jejich zálohování.

Zálohování musí být vyřešeno tak, aby bylo možné CDE a jeho obsah plnohodnotně obnovit:

- V průběhu Projektu, kdy je nutné zajistit v zásadě kontinuální dostupnost CDE a dat, Dodavatel umožní na vyžádání Objednatele přístup k této záloze do 3 pracovních dní.
- V případě neočekávaných událostí (selhání hardware, poškození dat, ztráta dat) zajistí Dodavatel do 3 pracovních dní bezztrátovou obnovu dat ze zálohy.
- Po ukončení a archivaci Projektu, například v případě požadavku na obnovení CDE pro výkon správy a údržby, rekonstrukce a opravy atp. (tzv. „archivní záloha"). Archivní záloha by měla obsahovat všechny dokumenty uložené k Projektu v CDE a zálohy všech databázových tabulek. Pokud Objednatel neurčí jinou formu exportu databázových dat (například konkrétní strukturu souborů MS Excel), poskytne Dodavatel schémata a popisy nutné k rekonstrukci databázových dat IT technikem třetí strany.

S ohledem na předpokládaný objem dat je žádoucí pro zálohování využívat formu automatických příp. poloautomatických záloh. Upřesňující požadavky může definovat Objednatel.

Záloha CDE musí být oddělena od primárních dat, tj. musí být v rámci infrastruktury uložená na odděleném místě nebo archivována na samostatném datovém nosiči (magnetická páska, pevný disk, NAS atp.), a to vždy při zachování plné důvěrnosti a bezpečnosti dat.

Dodavatel CDE musí mít definován plán záloh včetně definice postupů pro případ neplánovaného výpadku (disaster recovery). Tento plán záloh Dodavatel doloží Objednateli na vyzvání do 10 pracovních dní.

4 ZÁVAZNÉ ČÁSTI STRUKTUR CDE

Vlastní struktury podsložek, modulů, nebo jiný způsob organizace informací (např. podle metadat), musí respektovat procesní logiku a její vazby na používaná přístupová oprávnění. Proto se předpokládá jejich rozdělení na samostatné oblasti.

Rozdělení CDE na jednotlivé oblasti musí specifikovat Dodavatel. Současně musí Dodavatel připravit manuál použití CDE na Projektu.

Pro vytváření nových podsložek a jejich užívání musí Dodavatel stanovit závazná pravidla, jejichž účelem je zejména eliminovat riziko ohrožení funkčnosti CDE (např. použitím zcela nevhodných názvů, nebo překročením datové kapacity nebo jiným přetížením systému procesy pracovních složek). V nižších úrovních struktury se předpokládá možnost vytváření vlastních podsložek Dodavatelem, nebo jiných způsobů třídění (např. formou metadat), pro účely jejich interních agend spojených s Projektem.

5 ZABEZPEČENÍ DAT

5.1 BEZPEČNOSTNÍ POŽADAVKY

Musí být splněny následující bezpečnostní požadavky:

CDE 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.

CDE zaznamenává logy obsahující přihlašování/odhlašování uživatelů a umožňuje zástupcům Objednatele přístup k těmto informacím, které musí zahrnovat zejména časové razítko, přihlašovací jméno, IP adresu uživatele a popis události.

CDE zaznamenává logy řešení pro ochranu před škodlivým kódem, v případě webové aplikace také logy řešení pro ochranu webových aplikací.

CDE 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.

Dodavatel, nebo jím pověřená třetí osoba jako případný poskytovatel Cloud Computingu (služby CDE), 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 poskytovatele Cloud Computingu je osoba, která má sídlo v České republice a která je poskytovatele Cloud Computingu na základě plné moci zmocněná jej zastupovat.

Dodavatel musí zajistit na základě žádosti Objednatele bez zbytečného odkladu přístup k informacím a datům, které poskytovatel služby uchovává, včetně možnosti kontroly uchovávaných informací a dat v reálném čase.

Dodavatel musí zajistit řízení kontinuity činností v souvislosti s poskytovanou službou.

V případě vyžádání Objednatele podepíše Dodavatel dohodu o mlčenlivosti (NDA) týkající se dat uložených v CDE.

Dodavatel služby musí informovat o bezpečnostních událostech, které mohou mít vliv na integrity, důvěryhodnost a dostupnost uchovávaných dat a informací.

Dodavatel musí zajistit ochranu před škodlivým kódem nad poskytovatelem služby uchovávanými daty a informacemi.

Dodavatel musí zajistit ochranu webových portálů proti průnikům nasazením vhodné webaplikační ochrany (např. webaplikační firewall).

Řešení jako celek (všechny komponenty - OS, aplikace) musí být udržovány aktualizované a v případě zjištění specifické zranitelnosti aplikace musí být tato bezodkladně opravena.

Z pohledu důvěrnosti se s informací může seznámit pouze jakýkoliv zaměstnanec Objednatele, nebo jejich konzultanti a pověřené osoby, nebo osoby na straně Dodavatele. Ostatní osoby musí být schváleny Objednatelem.

Po skončení Projektu musí Dodavatel předat Objednateli digitální zálohu, nebo provozuschopná kopie CDE na paměťovém nosiči. V případě digitální zálohy musí tato záloha obsahovat veškerá data CDE exportované do adresářové struktury včetně logů, auditů a metadat.

5.2 ŘÍZENÍ PŘÍSTUPOVÝCH OPRÁVNĚNÍ

CDE musí umožňovat práci se skupinami uživatelů a přiřazování oprávnění těmto uživatelům.

CDE musí umožňovat přiřazování oprávnění na základě rolí (tyto role mohou být řešeny skupinami).

CDE musí zajišťovat řízení oprávnění a přístup k jednotlivým dokumentům na základě workflow.

CDE musí umožňovat generování souhrnných reportů obsahujících přehledu uživatelů, jejich přístupových práv, workflow a stavu workflow včetně asociovaných dokumentů.

5.3 FUNKCE MONITORINGU, AUDITU, SYSTÉMOVÝCH ZÁZNAMŮ AKTIVIT (LOG) APOD.

Musí být splněny následující požadavků na pořizování systémových záznamů aktivit (LOG):

- Systémové záznamy musí CDE pořizovat automaticky tak, aby nebylo možné v nich provádět jakékoli změny.
- Systémové záznamy musí být k dispozici všem subjektům užívajícím CDE a Dodavatel specifikuje způsob jejich poskytování.
- Systémové záznamy musí obsahovat druh provedené činnosti (nahrání, stažení nebo prohlížení záznamu, vložení poznámky, revize, redlining, změna stavu...).
- Systémové záznamy musí obsahovat datum a čas zaznamenané činnosti.
- Systémové záznamy musí obsahovat identifikaci původce zaznamenané činnosti.

5.4 DEFINICE PROCESŮ PROVÁDĚNÝCH V CDE (WORKFLOW)

CDE musí podporovat řešení pracovních postupů a procesů prostřednictvím workflow.

Procesy (workflow) musí být nastaveny v CDE Dodavatelem. Schémata jednotlivých procesů musí být zpracována Dodavatelem. Dále musí být na základě schémat procesů v CDE nastavena workflow formou šablon, které lze využít pro dílčí workflow.

CDE musí umožňovat realizaci po sobě jdoucích i paralelních kroků workflow.

Procesy probíhající na Projektu a digitalizované v CDE musí být Dodavatelem popsány formou procesních diagramů. Tyto procesní diagramy musí Dodavatel předložit do 5 pracovních dní před spuštěním CDE.

5.5 PROCESY SCHVALOVÁNÍ

Musí být nastaveny technické postupy užívané ke schválení dokumentů v digitální podobě. Např. schválení projektové dokumentace, vzorků výrobků a materiálů, postupu prací, zápisů a dalších procesů.

5.6 PROCESY PŘEDÁVÁNÍ, PŘEDÁVACÍ PROTOKOLY

Předávací protokoly musí být nastaveny jako šablony v CDE.

5.7 ZMĚNOVÁ ŘÍZENÍ, POŽADAVKY NA INFORMACE (TZV. RFI)

Změnová řízení a požadavky na informace musí být řešeny prostřednictvím workflow.

5.8 ŘEŠENÍ DALŠÍCH PROCESŮ

Distribuce zápisů z kontrolních dnů, schvalování postupů prací, vzorků, materiálů a výrobků, pokyny správce stavby musí být řešeny prostřednictvím workflow.

5.9 PŘIPOMÍNKOVÁNÍ DOKUMENTŮ V DIGITÁLNÍ PODOBĚ A ZPŮSOB VYPOŘÁDÁNÍ PŘIPOMÍNEK

CDE musí umožňovat digitální záznam připomínek k dokumentům.

Připomínky musí být možné zaznamenávat do jednotlivých souborů a přidávat revize těchto souborů do CDE nebo i jako součásti workflow.

Připomínky musí být možné zaznamenávat do workflow bez nutnosti vazby na jednotlivé dokumenty.

6 PODPORA PRO UŽIVATELE

6.1 UŽIVATELSKÉ NÁVODY A DALŠÍ ZDROJE INFORMACÍ

Dodavatel musí poskytnout uživatelské návody, manuály a další zdroje informací například formou odkazů na referenční příručky a uživatelské návody k softwarovým nástrojům CDE, a to jak přímo do CDE, kde budou tyto materiály uloženy jako samostatné dokumenty v digitální podobě, tak i emailem správci informací nebo jiné osobě určené Objednatelem.

6.2 PLÁN ŠKOLENÍ UŽIVATELŮ

Dodavatel musí zajistit zaškolení personálu Objednatele. V rámci školení musí být proškolena, mimo jiné, témata specifikovaná v rámci funkčních požadavků a workflow. Proškoleny musí být také vzorové postupy práce v rámci těchto funkčních požadavků a práce s dokumenty, s nimiž bude Objednatel v rámci CDE přicházet do styku.

6.3 ZAJIŠTĚNÍ PODPORY

6.3.1 Zajištění technické podpory

Dodavatel musí zajistit technickou podporu formou telefonické „hotline" pro určené osoby Objednatele v českém jazyce v pracovní dny 7:00 – 18:00.

Pro podporu mimo stanovenou dobu musí Dodavatel zajistit jiné vhodné způsoby kontaktování podpory (např. kontaktní e-mail).

Dodavatel musí uvést kontaktní osobu (osoby) poskytující technickou podporu spolu s telefonickým a emailovým spojením.

6.3.2 Zajištění uživatelské podpory

Dodavatel musí zajistit uživatelskou podporou dostupnou všem uživatelům (telefonicky/emailem/helpdesk), fungující minimálně v rozsahu denní pracovní doby 8:00 – 16:00.

Pro podporu mimo stanovenou dobu musí Dodavatel zajistit jiné vhodné způsoby kontaktování podpory (např. kontaktní e-mail).