Příloha A.II.

Požadavky na Společné datové prostředí (CDE)

–

Sanatorium Pálava

DIGITAL CONSTRUCTION CONSULTING

OBSAH

DIGITAL CONSTRUCTION CONSULTING

1 Seznam pojmů a zkratek

CDE – Společné datové prostředí (tzv. Common Data Environment)

IFC – otevřený datový formát a schéma (tzv. Industry Foundation Classes)

WF – digitální proces, někdy také nazýván jako „workflow“

Dokument - je každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či digitální, která byla vytvořena původcem nebo byla původci doručena

Field managment - nástroj pro koordinaci a řízení stavebních projektů přímo z místa stavby; umožňuje jejich přímou distribuci informací ze staveniště mezi účastníky projektu (např. při odstraňování vad a nedodělků)

Dokument v digitální podobě (DDP) - je dokument, jehož nosičem je datový soubor, nebo datová zpráva; digitální Dokument je v daném formátu a lze jej reprodukovat a zpracovat

SLA – představuje dohodu o úrovni poskytovaných služeb tzv. (Service Level Agreement) mezi Objednatelem a Zhotovitelm

Metadata - DDP popisných informací připojených k DDP; jiný výraz pro často používaný pojem „vlastnosti“; speciálním typem metadat je auditní log dokumentu

Dostupnost - udává, jaká je hodnota časové dostupnosti služby, např. 24/7/365–24 hodin, 7 dní v týdnu, 365 dní v roce

Incident - je takový stav, který neumožňuje provádět určité funkce, nebo nejsou splněny podmínky stanovené ve smlouvě

Požadavek - představuje jakýkoliv požadavek Objednatele služby, kromě Incidentu

Pokuta/Penále - určuje náhradu za vzniklý Incident, nebo za nesplnění doby odezvy, a nebo doby odstranění

Kontaktní osoby – kontakty na určené osoby Zhotovitele a Objednatele

Třetí strana – je právnickou, nebo fyzickou osobu, která v době uzavření smlouvy nemusí mít smluvní vztah s Objednatelem; může se jednat např. o zhotovitele stavby, koordinátora BOZP, TDI, správce stavby a další

Sandbox – je bezpečnostní mechanismus, který slouží pro oddělení běžících procesů a poskytuje omezený přístup ke zdrojům 5/21

Revize – je proces změny, při kterém se mění obsah dokumentu; výsledkem revize je nová Verze dokumentu

Verze – je jedna z několika podob téhož dokumentu/modelu, jde o číselné nebo jmenné označení stádia produktu.

2 Úvod

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, březen 2022 a Příloha č. 2 BIM

DIGITAL CONSTRUCTION CONSULTING

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.

Společné datové prostředí (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 Členy projektového týmu, jednoznačně určuje platnou verzi informace a pomáhá vyhnout se nedorozumění, duplicitám a chybám.

Úlohou systému CDE 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.

V dokumentu Plán realizace BIM (BEP), uvede Zhotovitel způsob a popis splnění požadavků v tomto dokumentu.

3 Systém CDE a funkční požadavky

3.1 SYSTÉM CDE

Objednatel využívá integrovaný jednotný systém CDE splňující požadavky uvedené v tomto dokumentu. Integrovaný jednotný systém CDE je takový systém, který spojuje všechny požadované funkce CDE do jednotného prostředí ovládaného přes jednotné rozhraní.

Zhotovitel má možnost připojit se ke stávajícímu řešení CDE Objednatele, kdy bude po celou dobu trvání projektu zajišťovat provoz tohoto CDE Objednatel. Zhotovitel takovém případě dostane přístupová práva po všechny zainteresované osoby, která mu zajistí Objednatel. V takovém případě Zhotovitel bude zastupovat roli uživatele s právy a povinnostmi Zhotovitele, jež jsou uvedené v tomto dokumentu.

Druhou možnost je, že Zhotovitel bude upřednostňovat vlastní řešení CDE (např. jiný dodavatel CDE než používá Objednatel). Tato varianta je možná pouze za podmínek, kdy Zhotovitel zajistí na vlastní náklady a vlastními prostředky plnou kompatibilitu obou systémů / aplikací CDE prostřednictvím API. Kompatibilita a práce s CDE se bude plně řídit pravidly uvedenými v tomto dokumentu, zejména oddíly 6.1 API rozhraní, 6.2 Technické řešení přístupu do CDE a navazujících. Zhotovitel nese plnou zodpovědnost za dostupnost jeho CDE řešení v souladu s tímto dokumentem.

Zhotovitel bude v rámci Společného datového prostředí udržovat aktuální Dokumenty, Digitální modely stavby, průzkumy, výkresy, vyjádření, dokumentace a další Dokumenty dle Smlouvy tak, aby byly k dispozici Objednateli.

Pokud bude mít CDE dodané Objednatelem integrovanou funkci umožňující práci s harmonogramy, je Zhotovitel povinen tuto funkčnost používat..

3.1.1 Funkční požadavky

1) Organizování DDP do složek (za složku jsou pro účely tohoto dokumentu považovány fyzické i virtuální složky).
2) Nahrání, sdílení DDP.
   a. Nahrávání jednotlivých DDP a složek.

DIGITAL CONSTRUCTION CONSULTING
dcc

b. Nahrání několika DDP a složek najednou (bulk upload).

c. Vkládání dalších informací k dokumentům v digitální podobě, tzv. metadat.

d. Zaznamenání minimálních metadat DDP a složek (datum poslední změny, autor změny DDP a složky, typ, velikost).

e. Sdílení jednotlivých či několika DDP a složek jednotlivým uživatelům a skupinám uživatelů.

3) Revize DDP včetně správy verzí.

a. Tvorba nové Verze dokumentu a její identifikace.

b. Možnost spravovat Verze DDP, vracet se k předchozím a aktivovat je jako nové verze.

c. Udržovat vazby na propojené dokumenty.

d. Revize DDP vnořených ve složkách (Revize celé adresářové struktury).

4) Stažení DDP a složek na úložiště mimo CDE.

a. Uložení DDP a libovolné adresářové struktury mimo CDE.

b. Stažení DDP a složek na úložiště mimo CDE musí být zaznamenáno v auditním logu.

5) Zobrazení nejčastěji požívaných formátů pro:

a. Textové dokumenty (.pdf, .txt).

b. Fotografie a jiné obrazové dokumenty (.jpg, .png,).

c. Digitální model stavby ve formátu IFC a umožnění manipulace s digitálním modelem stavby (dále viz kapitola „Práce s digitálním modelem stavby).

6) Audity dokumentů (např. formou audit logů) a dohodnutých procesů.

7) Vyhledávání v datech, včetně full-textového vyhledávání.

a. Vyhledávací mechanizmus CDE musí umožňovat vyhledávání dle vybraných kritérií v tomto rozsahu:

i. Vyhledávání podle připojených metadat k DDP (jedním z metadat je i název DDP).

ii. Vyhledávání v obsahu dokumentu. Jedná se o možnost vyhledávat uvnitř strojově čitelných DDP (MS Office dokumenty – .docx, .xlsx, .pptx, strojově čitelné PDF, textové DDP, .xml).

iii. Možnost sestavit vyhledávací dotaz pomocí podrobnějších vyhledávacích kritérií (rozlišení velkých/malých písmen, hledání klíčových slov v přesné a frázové shodě, chybějící slova, data a času).

iv. Filtrování dle metadat (např. dle stavu dokumentu, autora dokumentu či Revize apod.).

8) Podpora workflow – možnost tvorby WF (dále viz kapitola „Definice procesů prováděných v CDE (workflow)).

a. Tvorba lineárního workflow splňující základní požadavky na jednotlivé fáze dokumentů dle ISO 19650-1.

b. Tvorba nelineárního workflow, které umožňuje větvení, paralelní zpracování, případně skoky mezi fázemi.

c. Notifikace uživatelům při změně stavu dokumentu ve workflow.

9) Nastavitelné notifikace a upozornění uživatelů (na dokumenty, fáze workflow apod.).

10) Vytváření sestav nad daty uloženými v CDE (v minimální rozsahu: DDP, procesy, úkoly).

11) Nastavitelné skupiny uživatelů.

12) Zadávání úkolů a asociace DDP k těmto úkolům.

3.1.2 Práce s digitálním modelem stavby

V rámci CDE je nezbytné umožnit přímou interakci s digitálními modely stavby, které na sebe váží další informace. Propojení jednotlivých datových objektů uvnitř digitálních modelů staveb s dalšími informacemi uloženými v prostředí CDE tvoří jednu ze základních přínosů využití CDE.

1) Podpora práce s náhledem digitálního modelu stavby ve formátu ifc.

2) Zobrazení negrafických informací digitálního modelu stavby (např. názvy elementů a datových objektů a jejich vlastností).

3) Zobrazení/skrytí jednotlivých elementů a datových objektů digitálního modelu stavby.

4) Měření v digitálním modelu stavby včetně souřadnic.

5) Přidání metadat k elementům a datovým objektům digitálního modelu stavby. (V případě úpravy metadat zdrojového DDP digitálního modelu stavby, se na tento DDP nahlíží jako na novou verzi.)

6) Umožnění práce s tzv. field managmentem, tedy přijímat podněty, tikety a pracovat s nimiz aplikace přímo ze staveniště a umožnit prací s nimi pro všechny uživatele CDE.

3.1.3 Vazby mezi dokumenty v digitální podobě stavby

DDP mohou obsahovat vazby na jiné DDP. Tyto vazby mohou být zajištěny prostřednictvím externích referencí a hyperlinků (permanentních odkazů). CDE musí umožnovat pracovat s vazbami ve formátu hyperlinku. Použití ostatních typů vazeb je řešeno jinými softwarovými nástroji.

DIGITAL CONSTRUCTION CONSULTING

3.1.4 Datové formáty

Datové formáty DDP v CDE jsou pro účely metodiky rozděleny z hlediska funkcionality na kategorie podle typu DDP:

1) Office dokumenty

Běžnou součástí každého stavebního projektu jsou dokumenty MS OFFICE. Word (.docx) a Excel(.xlsx) a tvoří podstatnou část ukládaných dokumentů.

a. CDE musí umožňovat tyto dokumenty přímo prohlížet.

b. Volitelnou funkcionalitou CDE je možnost dokumenty přímo editovat a ukládat Revize bez nutnosti stažení.

2) Rastrové obrázky

a. Systém CDE musí umožnit prohlížení rastrových obrázků minimálně ve formátech:

.jpeg a .png.

b. Volitelnou funkcionalitou CDE jsou základní nástroje pro úpravu obrázků - otočení, přiblížení, oříznutí, přidávání tvarů, značek a textů.

3) Dokumentace ve 2D a 3D

a. CDE musí umožnit práci s digitálním modelem stavby ve formátu IFC.

b. Volitelnou funkcionalitou CDE je prohlížení a práce s některým z nativních formátů

DDP (.dwg, .dgn, . db1, .ndw, .rvt, .nwf, .nwd apod.).

4) PDF

a. CDE musí umožnit prohlížení dokumentů ve formátu PDF včetně běžných operací jako je otočení, přiblížení, přepínání stránek a další.

b. Volitelnými funkcemi jsou:

i. Možnost digitálního podepisování (včetně kvalifikovaného podpisu dle EIDAS).

ii. Anotace PDF.

iii. Editace těch PDF, která jsou k tomu určená (vyplňovací pole).

5) Ostatní DDP

a. CDE musí umožnit uložit a stáhnout jakýkoli DDP bez ohledu na jeho příponu a velikost.

b. Formát BCF musí být v CDE podporován ve formě dokumentu v digitální podobě.

3.1.5 Lokalizace do češtiny

1) CDE musí být kompletně lokalizováno do českého jazyka. V české jazykové verzi musí být i veškeré související materiály (manuály, nápověda apod.).

2) Přípustná je rovněž anglická lokalizace, avšak pouze v případě jednoznačné shody všech spolupracujících subjektů na jejím použití. Vždy však musí být k dispozici manuál v českém jazyce, a to minimálně v rozsahu popisu základní funkčnosti a obsluhy CDE.

3.1.6 Integrované CDE

Požadovanou variantou řešení je použití integrovaného systému CDE. Ten spojuje všechny funkce CDE do jednotného prostředí ovládaného přes jednotné společné rozhraní. Zhotovitel ve své nabídce vždy předloží popis nabízeného CDE a výslovně stanoví, že se jedná o integrované CDE. Objednatel může specifikovat, zda požaduje integrované, nebo modulární řešení. Jestliže Objednatel tuto specifikaci neuvede, předpokládá se, že je volba řešení na Zhotoviteli.

4 Požadované licence

Licence do CDE zajišťuje Objednatel.

V případě, že Zhotovitel bude chtít využít CDE vlastní, pak je povinen zajistit jeho kompatibilitu prostřednictvím API.

5 Přístupnost a dostupnost CDE

5.1 API ROZHRANÍ

API rozhraní z anglického (Application Programable Interface) je rozhraní pro výměnu dat mezi aplikacemi. Rozhraní obsahuje jednoznačně zdokumentované tzv. "koncové body." Objednatel poskytne Zhotoviteli do 14 dní od vyžádání specifikaci API CDE Objednatele.

1) CDE musí disponovat API minimálně v rozsahu zabezpečující funkčnost (minimální funkční požadavky) dané tímto dokumentem.

2) Zhotovitel jako součást Plánu realizace BIM předloží dokumentaci API dodávaného systému. Dokumentace musí být popsána do takové podrobnosti, že třetí straně umožní propojení vlastního CDE na CDE poskytnutého Zhotovitelem.

3) Pro ověření funkčnosti API a zajištění propojení si může Třetí strana vyžádat přístup do CDE poskytnutého Zhotovitelem. Zhotovitel je povinen tento přístup umožnit.

5.2 DOSTUPNOST CDE

1) Zhotovitel zajistí nepřetržitou dostupnost, provozuschopnost a údržbu systému. V případě nefunkčnosti/nedostupnosti systému (mimo plánovaná servisní okna dle platné smlouvy) garantuje Zhotovitel jeho opětovné zprovoznění dle kapitoly Podpora pro uživatele od telefonického/e-mailového/ nahlášení nefunkčnosti/nedostupnosti systému Objednatelem nebo jakoukoliv pověřenou osobou daného projektu. Dodavatel systému garantuje provoz systému (poskytne klientovi odezvu) minimálně 99 % času z celkového času objednávky mimo servisní okna.

2) Objednatel požaduje systém s garantovaným nepřetržitým servisem (24/7).

3) Zhotovitel podrobně specifikuje způsob řešení nezbytných technických zásahů do systému, které mohou vést k výpadkům funkčnosti, způsob řešení technických závad a minimalizace jejich dopadů na CDE v Plánu realizace BIM (BEP).

4) Objednatel požaduje Dostupnost CDE na dobu trvání smluvního vztahu prodlouženou o tři měsíce.

DIGITAL CONSTRUCTION CONSULTING
dcc

5.3 ZÁLOHOVÁNÍ DAT CDE

1) Dodavatel CDE systému musí deklarovat bezpečnost uložených dat, jejich Dostupnost a zajistit jejich zálohování. Zálohování musí být vyřešeno tak, aby bylo možné CDE a jeho obsah plnohodnotně obnovit:

a. V průběhu projektu, kdy je nutné zajistit v zásadě kontinuální Dostupnost CDE a dat Zhotovitel umožní na vyžádání Objednatele přístup k této záloze.
b. V případě neočekávaných událostí (selhání hardware, poškození dat, ztráta dat) zajistí Zhotovitel do tří pracovních dnů bezztrátovou obnovu dat ze zálohy.
c. Po ukončení a archivaci projektu, například v případě požadavku na obnovení CDE pro výkon správy a údržby, rekonstrukce a opravy apod. (tzv. „archivní záloha“). Archivní záloha by měla obsahovat všechny dokumenty uložené k danému projektu v CDE a zálohy všech databázových tabulek. Pokud objednatel neurčí jinou formu exportu databázových dat (například konkrétní strukturu DDP MS Excel), poskytne Zhotovitel schémata a popisy nutné k rekonstrukci databázových dat IT technikem třetí strany.

2) S ohledem na předpokládaný objem dat je žádoucí pro zálohování využívat formu automatických případně poloautomatických záloh. Upřesňující požadavky definuje objednatel.

3) 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.

4) Doporučuje se, aby měl Zhotovitel pro CDE definován plán záloh včetně definice postupů pro případ neplánovaného výpadku (Disaster Recovery). Upřesňující požadavky definuje objednatel.

Dodavatel je povinen předat zálohu dat na datovém nosiči Objednateli do 15 pracovních dní od výzvy Objednatele.

6 Pravidla pojmenování složek a dokumentů v digitální podobě

6.1 PRAVIDLA POJMENOVÁNÍ SLOŽEK A DOKUMENTŮ V DIGITÁLNÍ PODOBĚ

1) Povinná pravidla pro pojmenování složek a dokumentů v digitální podobě (DDP):

a. Délka názvu jednoho DDP či složky maximálně 256 znaků dle standardu Windows.
b. V názvech nejsou povoleny zakázané znaky Windows (např. / : * ? " < > |).

2) V případě, že Objednatel disponuje vlastním předpisem upravujícím pojmenování dokumentů v digitální podobě a požadavky na složkovou strukturu, uvede Objednatel tyto požadavky v tomto odstavci.

3) Doporučená pravidla pro pojmenování dokumentů v digitální podobě:

V rámci projektu zpracovávaného dle metodiky BIM musí být jmenná konvence pro názvy dokumentů (popř. i složek) stanovena v požadavcích Objednatele na data, nebo Dokumentu BEP. CDE systém musí podporovat možnost zadat pravidla pojmenování dokumentů dle BEP přímo do systému. Jedná se převážné o strukturu a názvy složek a pojmenování dokumentů v digitální podobě. Nastavitelné parametry názvů složek a dokumentů:

i. Délka názvu.
ii. Formát názvu (písmena, číslice, maska znaků – přednastavený formát názvu).

DIGITAL CONSTRUCTION CONSULTING

6.2 PRAVIDLA PRO VERZOVÁNÍ DDP

1) Dokument musí být v systému CDE uložen vždy pouze jednou a na jednom místě, jeho nové verze (Revize) jsou vkládány jako jeho další verze nikoliv jako samostatné dokumenty s jiným názvem a v jiném umístění. Původní Verze dokumentu vždy musí být v CDE ponechána v nezměnitelné podobě včetně všech jejich vlastností.

2) Konkrétní pravidla pro verzování dokumentů v digitální podobě definuje pro konkrétní CDE dodavatel v Plánu realizace BIM (BEP).

6.3 PRAVIDLA PRO NAKLÁDÁNÍ S DDP

1) U dokumentů v digitální podobě musí být stanovena pravidla pro omezení jejich maximální velikosti a způsobu rozdělení velkých DDP na menší tak, aby splnila všechny požadavky Objednatele. Doporučuje se požadovat:

2) Maximální velikost jednoho DDP ve formátu IFC do 1 GB.

3) Maximální velikost jednoho DDP ve formátu PDF do 100 MB.

4) Dodavatel neručí za integritu a bezpečnost dat po přenesení dokumentu v digitální podobě mimo CDE.

7 Definice procesů prováděných v CDE (WORKFLOW)

7.1 FUNKČNÍ POŽADAVKY NA PROCESY

Workflow (pracovní tok) je sekvence aktivit a jejich stavů, které popisují pracovní postup. V CDE musí být nástroj pro aplikaci nebo tvorbu workflow, které podpoří digitální proces pro pracovní postupy definované organizací.

1) CDE musí umožnit nadefinovat workflow pro Objednatelem požadované úlohy a také umožnit vytváření vlastních workflow, podle potřeb jednotlivých organizací na procesní toky.

2) CDE musí umožnit definovat základní workflow pro typické úlohy v daném odvětví a stupni projektu. Definice skupin uživatelů, včetně sekvence aktivit a jejich stavů je na Objednateli.

3) Tvorba libovolného množství jednotlivých aktivit a stavů pracovního toku.

4) Tvorba sériového workflow. Tzn. definovat jednotlivé aktivity pracovního toku, které na sebe navazují a zajistit přechod z jedné aktivity a jejího stavu do následující nebo předchozí aktivity.

5) Tvorba paralelního workflow, kdy může docházet k větvení procesů na základě kritérií a může docházet k souběžnému zpracování více aktivit na jednou.

6) Úprava vlastností pracovního toku a přidání dalších aktivit.

7) Spojování aktivit do pracovního toku sériového nebo paralelního.

8) Definovat přístupová práva podle rolí v projektu na každou aktivitu pracovního toku.

9) Nástroje pro notifikaci při změně stavu (aktivity).

10) Prostřednictvím oprávnění řídit přístup k DDP na základě probíhajícího workflow.

11) Zaznamenávat změny stavů workflow (např. schválení, připomínky).

12) Přidávat informované osoby, které mohou v rámci aktivity pracovního toku nahlížet do dokumentů.

13) Umožnit nastavení termínů pro jednotlivé aktivity workflow.

14) Umožnit automatické uzavření vybraných workflow v návaznosti na termíny.

15) Umožnit přidání textové poznámky k vybraným workflow.

16) Umožnit přidání DDP k vybraným aktivitám workflow.

8 Zabezpečení dat v systému

8.1 ŘÍZENÍ PŘÍSTUPOVÝCH OPRÁVNĚNÍ

1) Systém CDE musí umožnit řídit uživatelská oprávnění do jednotlivých částí projektu i modulů CDE (dokumenty, procesy, modely apod.) a musí toto umožnit hromadně přiřazením uživatele do jedné nebo několika skupin.

2) Systém CDE musí poskytovat komplexní moderní zabezpečení dat a přístupů. Musí se řídit platnou českou i evropskou legislativou, zejména zákonem o kybernetické bezpečnosti 181/2014 Sb.

8.1.1 Seznam uživatelů, skupin, rolí apod.

1) Systém CDE musí umožnit řídit uživatelská oprávnění do jednotlivých částí projektu i modulů CDE (dokumenty, procesy, modely apod.) a musí toto umožnit hromadně přiřazením uživatele do jedné nebo několika skupin.

2) Systém CDE musí poskytovat komplexní moderní zabezpečení dat a přístupů. Musí se řídit platnou českou i evropskou legislativou, zejména zákonem o kybernetické bezpečnosti 181/2014 Sb.

8.1.2 Schéma nastavení práv podle struktury uložiště

1) Systém CDE musí umožnit řízení oprávnění i do dílčích částí jednotlivých subsystémů, v případě DDP se jedná o:

a. Přístup (čtení) k jednotlivým adresářům a nastavení možnosti do nich zapisovat.

b. Možnost měnit dokumenty jiných uživatelů.

c. Možnost vidět Verze dokumentů.

d. Možnost revidovat dokument.

e. Možnost nastavení přístupů k jednotlivým projektům a částem projektů (moduly).

8.2 BEZPEČNOSTNÍ POŽADAVKY

Dodavatel systému CDE musí být certifikován podle normy ČSN ISO/IEC 27001. Systému musí plnit zejména tyto požadavky na bezpečnost:

a. Zabezpečení všech dotazů (vyjma přihlášení).

b. Přenos dat o kontextu uživatele pomocí autorizačních tokenů.

c. Komunikace přes zabezpečený protokol HTTPS.

DIGITAL CONSTRUCTION CONSULTING

d. Systém nesmí ukládat uživatelská hesla na straně serveru v otevřené podobě.

e. Možnost vícefaktorového ověření.

f. Na klientské straně, pokud jsou uloženy přístupové údaje, musí k tomu být využity zabezpečené prostředky (např. Windows Vault nebo manager hesel internetového prohlížeče).

g. Hesla uživatelů musí vyžadovat splnění požadavků pro silná hesla.

h. Pokud se jedná o desktopového klienta k CDE, musí být aplikace digitálně podepsána certifikátem vystaveným důvěryhodnou certifikační autoritou.

i. CDE musí poskytovat kontinuální zálohy databázových informací s možností obnovit data v dílčím čase.

j. Umístění serverů v zabezpečeném komplexu

   i. Omezený přístup.

   ii. Kamerový systém.

   iii. Protipožární ochrana.

   iv. Duální připojení k internetu pro případ výpadku jedné z větví.

   v. Duální napájení - připojení zákaznické technologie k druhé větvi elektrické energie.

k. Administrátorské přístupy k databázím a aplikačním serverům mají pouze osoby, které mají smluvně danou mlčenlivost.

l. Ochrana proti DDoS (Distributed Denial of Service Attack).

m. Ochrana proti Cross-site Scripting.

n. Ochrana proti SQL Injection.

o. Ochrana proti Man-in-the-middle útokům.

8.3 FUNKCE MONITORINGU SYSTÉMOVÝCH ZÁZNAMŮ AKTIVIT

1) CDE musí umožnit monitorovat běh databázových a výkonných částí systému (tzv. aplikačních serverů) a Dostupnost systému.

2) CDE musí umožnit monitoring síťového provozu a potenciálních hrozeb a útoků ze strany internetu. Dále auditovat všechny uživatelské akce, které jsou prováděny vzhledem k serverové části CDE (např. stažení DDP, nahrání DDP, založení projektu, neúspěšné přihlášení apod.).

3) CDE musí v rámci auditní stopy ukládat minimálně tato data:

a. Původce akce (identifikátor uživatele).

b. Čas akce, včetně časového pásma.

c. Typ akce a parametry.

Tento dokument byl vytvořen na základě standardů ČAS a SFDI pro účely projektu a jedná se o autorské dílo zpracovatele. Není dovoleno tento text, ani jeho části, upravovat, kopírovat nebo jakkoli měnit bez souhlasu autora.

Anthony Christian Joël De Busschere [redacted]

Ing. Jan Kodytek [redacted]

Ing. Zdeněk Pokorný [redacted]

Martin Horák [redacted]

Mgr. Jan Grolich [redacted]

DIGITAL CONSTRUCTION CONSULTING