**PŘÍLOHA Č.3 – TECHNICKÁ SPECIFIKACE SYSTÉMU CDE**

1. **Funkční požadavky** 
   1. **DMS (Document management system)** 
      1. **CDE** bude obsahovat adresářově orientovaný systém dokumentů, dle práv bude umožněno vytváření složek a podsložek pro každý projekt individuálně.
      2. S dokumenty bude možné nakládat obdobně, jako například v Průzkumníku v MS Windows, nebo obdobných systémech (vkládání, přesouvání nebo vyřazení dokumentů, atd).Bude možné provádět základní úkony nad souborem/soubory, tak i adresářem/adresáři. Mezi běžné úkony patří:
         1. stáhnout/sdílet/otevřít,
         2. vkládat komentáře /připomínky (formáty MS Office a \*.pdf),
         3. sledovat (například nastavit notifikace, pokud se se souborem děje nějaká aktivita),
         4. vyřadit s možností obnovy administrátorem.
      3. V **CDE** bude možné otevírat a prohlížet běžné grafické i textové formáty (\*.jpeg, \*.png, \*bmp, \*.dwg, \*.rvt, \*.dgn, \*.ifc, \*.txt, \*.pdf, formáty MS Office atd).
      4. **CDE** bude umožňovat zobrazit detail dokumentu, který bude obsahovat např. náhled dokumentu, autora dokumentu, verzi/verze, stav revizí (workflow) a aktivit nad dokumentem, data posledního použití, sdílení atd.
      5. Soubory bude možné rozšiřovat o další informace, tzv metadata (kategorie, atributy, poznámky atd). Na základě těchto metadat bude možné filtrování a vyhledávání v souborech.
      6. Dokumenty budou v **CDE** uloženy vždy jen jednou, **CDE** umožní jejich automatické verzování. Revize dokumentů budou ukládány jako verze původního souboru automaticky v rámci **CDE** (původní soubor bude vždy nahrazen novým s tím, že systém **CDE** automaticky zaznamená, že se jedná o novou revizi dokumentu).
      7. **CDE** umožní porovnávání verzí dokumentů jak textových, tak grafických (např. soubory ve formátech \*.pdf, MS Office, \*.ifc, dwg. atd.) a možnost zobrazení všech předchozích verzí dokumnetů. Porovnání bude indikovat přidané a odebrané prvky, změnu geometrie, změnu hodnot parametrů u prvků modelu.
      8. Soubory bude možné sdílet se členy projektu, nebo jen formou odkazu dalším stranám.
   2. **Workflow WF (oběh dokumentů, schvalovací procesy, projednávání)**
      1. **CDE** umožní nastavit individuální proces WF nad jednotlivými dokumenty, nebo celými složkami dokumentů.
      2. Každé WF bude samostatné vlákno, které bude možné dále kategorizovat za účelem dalšího filtrování a vyhledávání.
      3. WF bude spouštěno pomocí libovolně definovatelných šablon.
      4. Jednotlivé kroky WF budou adresné na uživatele/roli, který má dané téma řešit, a bude možné nastavit termín pro odpověď/řešení.
      5. Ve zvoleném kroku WF bude moci být jedna, nebo více osob, přičemž ke schválení bude možno nastavit pouze jednu z nominovaných osob, nebo různé varianty. Bude umožněna zastupitelnost.
      6. Jednotlivé kroky WF umožní minimálně schválení, zamítnutí, přidání souborů, poznámek, náhledy na dokumenty, otevření dokumentu atd.
      7. Veškerá aktivita v rámci WF musí být plně logována včetně času, uživatele atp.
      8. Informace o WF budou zasílány pomocí notifikací do e-mailu nastavených uživatelů, nebo uživatelů zúčastněných ve WF, zároveň budou zobrazeny na dashboardu nebo v uživatelském prostředí daného uživatele.
      9. V **CDE** musí být zajištěn proces popsaný v ČSN EN ISO 19650 tj. pracovat se základními stavy dokumentů - rozpracováno / sdíleno / publikováno / archivováno.
      10. V **CDE** bude přehledný seznam všech WF běžících v daném projektu.
      11. **CDE** umožní evidenci vad a nedodělků (samostatným modulem, nebo formou úkolů).
      12. **CDE** umožní export zadaných úkolů.
   3. **Vyhledávání** 
      1. **CDE** bude umožňovat fulltextové vyhledávání v názvech složek i dokumentů.
      2. **CDE** umožní fulltextové vyhledávání uvnitř dokumentů (zejména v souborech ve formátech MS Office a \*.pdf).
      3. **CDE** bude obsahovat filtry, včetně definování uživatelských filtrů a následně také hromadný výběr.
   4. **Zobrazení a práce s  daty digitálního modelu stavby (DIMS)**

* + 1. **CDE** bude obsahovat integrovanou prohlížečku grafických dat bez nutnosti stažení a otevření dat mimo **CDE**.
    2. **CDE** umožní vytváření řezů, nebo řezového kvádru v modelu.
    3. **CDE** umožní měření vzdáleností, úhlů, ploch a objemů v modelu.
    4. **CDE** umožní zobrazení negrafických informací prvků.
    5. **CDE** umožní připomínkovat /komentovat prvky v modelu.
    6. **CDE** umožní zobrazení sdruženého/federativního modelu a spojení více modelů v prostředí **CDE**.
    7. **CDE** umožní zobrazit/skrýt prvky a datové objekty modelu.
    8. **CDE** umožní nastavení průhlednosti prvků a datových objektů.
    9. **CDE** umožní vyhledávání prvků uvnitř modelu.
  1. **Dashboardy**
     1. **CDE** umožní dashboard pro každý projekt.
     2. Dashboard bude zobrazovat základní data projektu, notifikace, schvalovací procesy, úkoly.
  2. **Další funkce**
     1. **CDE** bude obsahovat systém notifikací, které přes uživatelksé centrum nebo formou e-mailu informují definované uživatele o potřebě aktivity, nebo o aktivitě, která se v **CDE** udála.
     2. **CDE** umožní hromadné stažení zvolených dokumentů včetně adresářové struktury bez omezení velikosti souborů.

1. **Bezpečnostní požadavky**
   1. **Práva a přístupy**
      1. **CDE** musí obsahovat systém oprávnění a udělování přístupů do složek, včetně definování uživatelských rolí.
      2. Systém přístupů a oprávnění musí být řízen administrátorem projektu, který bude po zaškolení plně na straně Dodavatele.
      3. Systém oprávnění musí být tak variabilní, aby umožnil udělit specifická práva a přístupy na jednotlivé adresáře a podadresáře pro jednotlivé uživatele nebo role.

# **Logování**

* + 1. **CDE** musí zaznamenávat přihlášení i odhlášení jednotlivých uživatelů.
    2. **CDE** musí zaznamenávat kompletní časově neomezenou historii kroků všech administrátorů i uživatelů. Krokem je myšlen podstatný úkon s vlivem na data, metadata, nebo procesy, jako například úkony copy/move/delete/rename/download/upload/modify nebo u schvalování schválení/zamítnutí/poznámky/odeslání do schvalování atd.
    3. Zaznamenané kroky musí obsahovat minimálně čas a uživatele, který krok udělal.
    4. U každého souboru nebo WF tak musí být dohledatelná kompletní historie včetně času.
    5. Logy musí být možné exportovat do .csv, nebo obdobného formátu.
    6. Logy nemůže modifikovat nebo smazat ani administrátor.

# **Požadavky na splnění technických norem, požadavků a metodik**

* + 1. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
    2. zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů.
    3. 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) do 30/06/2024, následně Vyhláška č. 360/2023 Sb.
    4. zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce;
    5. 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).
    6. Nařízení Evropského parlamentu a rady (EU) 2016/679, obecné nařízení o ochraně osobních údajů (např. dodržením ISO 27001).

# **Technické požadavky**

* + 1. **CDE** bude přístupné minimálně v nejčastěji používaných webových prohlížečích ve své aktuální verzi (např. Firefox, Chrome, Safari, Edge nebo jiné) bez nutnosti instalací dalších komponent a bude poskytovat responsivní rozhraní.
    2. Velikost datového prostoru **CDE** nebude omezena.
    3. **CDE** může pro prohlížení a otevírání souborů využívat aplikace 3. stran, jejichž licence však budou poskytnuty v rámci pořízení **CDE**, např. využití integrované prohlížečky souborů modelů jiného **Poskytovatel CDE** e mimo **CDE**.
    4. Pro přihlášení do **CDE** bude možné nastavit multifaktorové přihlášení (např. přes telefon).
    5. Dodání, nastavení a zprovoznění systému **CDE** bude v IT prostředí **Poskytovatele CDE** včetně automatizovaného zálohování do off-site lokace s minimální frekvencí 1x 8 hodin.
    6. Pro práci v prostředí **CDE** nebude nutná desktopová aplikace, **CDE** musí být přístupné i z mobilních zařízení (tablet, smartphone, a to jak s OS Android, tak iOS). Není nutná mobilní verze aplikace, ale minimálně responsivní prostředí je požadováno.
    7. **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.
    8. **CDE** bude plně lokalizované do českého jazyka, vč. zákaznické podpory.
    9. Po ukončení smlouvy, případně na základě pokynu zadavatele, musí **Poskytovatel CDE** zajistit export DMS a odchod organizace z hostingu do svého prostředí.
    10. **Poskytovatel CDE** musí při ukončení smluvního vztahu zajistit bezpečnou likvidaci dat a bezpečnou likvidaci kryptografických klíčů, které šifrují zákaznický obsah v úložištích, v souladu s vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti.
    11. **Poskytovatel CDE** má sídlo nebo bydliště v členském státu Evropské unie nebo má určeného svého zástupce ve členském státu Evropské unie obdobně podle čl. 27 obecného nařízení o ochraně osobních údajů.
    12. **Poskytovatel CDE** má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí a umožní zpřístupnění vzdáleně všech událostí týkajících se konkrétního zákazníka zákazníkovi, bez zbytečného prodlení po vzniku události.
    13. **Poskytovatel CDE** garantuje, že primární a alespoň jedno záložní datové centrum, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra, je v dostatečné vzdálenosti od přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka vedoucích k narušení nebo omezení poskytování služby nebo bezpečnosti informací.
    14. **Poskytovatel CDE** garantuje dostupnost služby s provozní dobou 24x7 alespoň v úrovni 95 % vyhodnocované na měsíční bázi včetně časů nutných pro servisní zásahy.
    15. **Poskytovatel CDE** na vyžádání předloží doklady o provádění pravidelných penetračních testů v posledncíh 3 letech. Způsob provedení testů musí odpovídat metodice OWASP.

# **Obecné požadavky**

* + 1. Vzhledem k povaze činnosti a majetku Zadavatele je nutné brát v úvahu požadavky, především bezpečnostní. Dle povahy projektu a stavby bude nutné zvážit, v jakém režimu bude povolen přístup k datům. To vytváří nároky na velmi kvalitní a podrobné nastavení práv. Práva musí být velmi variabilní, nastavení přístupu musí být jak na roli, tak osobu. Přístup musí být možné nastavit minimálně na adresář a to nic/čtení/zápis/administrator.
    2. Zároveň nesmí být možné soubory z **CDE** trvale smazat, toto právo nebude vyhrazeno ani administrátorovi zadavatele.

**PŘÍLOHA Č.3 – BEZPEČNOSTNÍ POŽADAVKY**

Za účelem plnění povinností stanovených Zadavatelem jakožto povinné osobě ve smyslu vyhlášky 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), je **Poskytovatel** **CDE** povinen plnit níže uvedené povinnosti zejm. součinnostního a bezpečnostního charakteru.

**Poskytovatel** **CDE** je povinen plnit relevantní povinnosti v rozsahu a způsobem, aby byl naplněn účel právní úpravy v oblasti bezpečnostních opatření, kybernetických bezpečnostních incidentů, reaktivních opatření, náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat ve vztahu k povinnostem, které tato právní úprava stanovuje Zadavateli jakožto povinné osobě dle předpisů z oblasti kybernetické bezpečnosti, a to i v případě změny příslušné právní úpravy. V takovém případě je Zadavatel oprávněn požadovat od **Poskytovatele** **CDE** přiměřenou součinnost i nad rámec povinností stanovených v těchto požadavcích, avšak vždy pouze za účelem zajištění plnění povinnosti **Poskytovatelem** **CDE** z oblasti kybernetické bezpečnosti ve smyslu shora uvedeného.

**§ 3 Systém řízení bezpečnosti informací**

**Poskytovatel CDE**  se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 3 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále jen „VKB“), které musí splnit Zadavatel. Minimálně se **Poskytovatel CDE** zavazuje v rozsahu předmětu plnění na své straně:

* + 1. Prosadit bezpečnostní zásady a procesy, které budou pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně **Poskytovatele CDE** při poskytování předmětu plnění.
    2. Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je, vyhodnocovat jejich účinnost.
    3. Vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaného předmětu plnění, zaznamenávat veškeré podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na vyžádání tyto záznamy Zadavateli zpřístupnit.
    4. Stanovit a udržovat aktuální bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně **Poskytovatele CDE** při poskytování předmětu plnění. Bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací.
    5. Stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky.

**§ 4 Řízení aktiv**

**Poskytovatel CDE** se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 4 VKB, které musí splnit Zadavatel. Minimálně se **Poskytovatel CDE** zavazuje v rozsahu předmětu plnění na své straně:

1. Stanovit a udržovat rozsah a seznam aktiv využívaných pro plnění této smlouvy (aktivy se rozumí např. data a informace k předmětu plnění dle této smlouvy, systémy ICT, moduly, HW prvky - infrastruktura hlasové a datové komunikace, aplikace, databáze, servery, úložiště, koncová zařízení – pracovní stanice typu osobní počítač nebo notebook, mobilní koncová zařízení – přenosná zařízení typu telefon, tablet, notebook, netbook, PDA, apod.), a tato aktiva strukturovaně popsat a Zadavateli předložit na vyžádání do třiceti (30) dnů, a to po celou dobu trvání smlouvy a do dvou (2) let po jejím ukončení.

**§ 6 Organizační bezpečnost**

**Poskytovatel CDE** se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 6 VKB, které musí splnit Zadavatel. Minimálně se **Poskytovatel CDE** zavazuje v rozsahu předmětu plnění na své straně:

1. Jmenovat nejpozději do pěti (5) dnů po uzavření této Smlouvy odpovědnou kontaktní osobu pro potřeby zajištění plnění těchto kybernetických požadavků a související komunikaci mezi Smluvními stranami (dále také jen „Kontaktní osoba“). Kontaktní osobu sdělí **Poskytovatel CDE** písemně Zadavateli v téže lhůtě. Zadavatel stanovuje, že určení Kontaktní osoby pro bezpečnost na straně **Poskytovatele CDE** nemá dopad na ustanovení Smlouvy týkající se odpovědných osob ve věcech smluvních a technických.
2. Využívat pro poskytování předmětu plnění pouze oprávněných osob, které byly řádně seznámeny příslušnými ustanoveními interních řídících aktů Zadavatele a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu plnění.

**§ 8 Řízení dodavatelů**

**Poskytovatel CDE** se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 8 VKB, které musí splnit Zadavatel. Minimálně se **Poskytovatel CDE** zavazuje v rozsahu předmětu plnění na své straně:

1. Využívá-li při poskytování předmětu plnění **Poskytovatel CDE**, zajistit adekvátní dodržování kybernetických požadavků rovněž ve smluvních vztazích se svými **Poskytovateli CD**, přičemž tuto skutečnost se **Poskytovatel CDE** zavazuje doložit Zadavateli do deseti (10) pracovních dnů od podpisu příslušné Smlouvy, na jejímž plnění se budou **Poskytovatelé CDE** podílet, písemné prohlášení o dodržování kybernetických požadavků u svých **Poskytovatelů CDE**.
2. Pokud při poskytování předmětu plnění dochází ke zpracování osobních údajů, zajistit uzavření samostatných smluv (tj. smluv se svými **Poskytovateli CDE**, zaměstnanci a případnými dalšími osobami podílejícími se na poskytování plnění z této smlouvy) ve smyslu příslušných ustanovení Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a zákona č. 110/2019 Sb., o zpracování osobních údajů, v platném znění.

**§ 10 Řízení provozu a komunikací**

**Poskytovatel CDE** se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 10 VKB, které musí splnit Zadavatel. Minimálně se **Poskytovatel CDE** zavazuje v rozsahu předmětu plnění na své straně:

1. Zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění.
2. Na vyžádání poskytnout Zadavateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře.
3. Zajistit, že pro poskytování předmětu plnění budou využívány pouze aplikace a technologie, které jsou v souladu s platnou českou a evropskou legislativou, především s ohledem na licenční podmínky a Autorský zákon AZ.

**§ 14 Zvládání kybernetických bezpečnostních událostí a incidentů**

**Poskytovatel CDE** se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 14 VKB, které musí splnit Zadavatel. Minimálně se **Poskytovatel CDE** zavazuje v rozsahu předmětu plnění na své straně:

1. Stanovit a popsat na své straně činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání bezpečnostních incidentů.
2. Bez zbytečného odkladu hlásit Zadavateli všechny bezpečnostní události a incidenty s potenciálním negativním dopadem na Zadavatele, a to stanoveným komunikačním kanálem nebo prostřednictvím Kontaktní osoby.
3. Vyhodnocovat informace o bezpečnostních incidentech a uchovávat je pro budoucí použití s ohledem na požadavky platné české a evropské legislativy.
4. V případě vzniku bezpečnostní události a následného zvládání a vyhodnocování bezpečnostního incidentu a/nebo v případě podezření na bezpečnostní incident poskytnout Zadavateli aktivní součinnost a relevantní informace o podezřelém zařízení či osobě na straně **Poskytovatele CDE**.
5. Bez zbytečného odkladu a po dohodě s Zadavatelem realizovat opatření požadovaná Zadavatelem v dohodnutých termínech ke snížení dopadu bezpečnostního incidentu nebo zamezení pokračování incidentu.
6. Spolupracovat při analýze příčin bezpečnostního incidentu a navrhnout opatření s cílem zamezit jeho opakování v případě, že **Poskytovatel CDE** bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

**Poskytovatel CDE**  bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení kybernetických požadavků, jehož příčina je na straně **Poskytovatele CDE**, nebude posuzován jako okolnost vylučující odpovědnost **Poskytovatele CDE** za prodlení s řádným a včasným plněním předmětu této smlouvy a nebude důvodem k jakékoli náhradě případné újmy **Poskytovatel CDE** i či jiné osobě ze strany Zadavatele. Ostatní ustanovení ohledně odpovědnosti **Poskytovatele CDE** za prodlení obsažená v této Smlouvě nejsou tímto ustanovením dotčena.

**§15 Řízení kontinuity činností**

**Poskytovatel CDE** se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 15 VKB, které musí splnit Zadavatel. Minimálně se **Poskytovatel CDE** zavazuje v rozsahu předmětu plnění na své straně:

1. Zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění.
2. Pravidelně kontrolovat a testovat, že je schopen kontinuitu aktiv zajistit dle sjednané úrovně služeb.

**§ 18–27 Bezpečnostní nástroje**

**Poskytovatel CDE** se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 18 až § 27 VKB, které musí splnit Zadavatel. Minimálně se **Poskytovatel CDE** zavazuje v rozsahu předmětu plnění na své straně:

1. Realizovat bezpečnostní opatření pro odstranění nebo blokování síťového spojení/síťových spojení, které/která neodpovídají požadavkům na ochranu integrity komunikační sítě.
2. Průběžně zaznamenávat a uchovávat data o provozu zařízení ICT (provozní a lokalizační údaje) v rozsahu předmětu plnění a v souladu s požadavky platné české a evropské legislativy.
3. Na vyžádání poskytnout Zadavateli report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu předmětu plnění, a to po celou dobu trvání Smlouvy a do dvou (2) let po jejím ukončení.
4. Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění a ochranu získaných informací před jejich neoprávněným čtením nebo změnou.
5. Pro on-line transakce realizované prostřednictvím webových technologií implementovat TLS/SSL certifikáty s cílem zajistit jejich důvěrnost, integritu a identitu komunikujících protistran.
6. Veškeré neveřejné informace poskytnuté Zadavatelem chránit vhodným šifrováním a proti neautorizovanému přístupu.