Smlouva na Rozvoj a údržbu DMS v letech 2021 – 2025

č. sml. Zadavatele: ČÚZK-07686/2021

č. sml. Dodavatele: 018/2021

Smluvní strany:

Česká republika - Český úřad zeměměřický a katastrální

sídlo: Pod sídlištěm 1800/9, Kobylisy, 182 11 Praha 8
IČO: 00025712
DIČ: není plátce
ID datové schránky: uuaaatg
jejímž jménem jedná: [redacted] místopředseda
(dále jen „Zadavatel“)

a

CCA Group a.s.

sídlo: Karlovo nám. 288/17, 120 00 Praha 2
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn. B5556
IČO: 25695312
DIČ: CZ25695312
bankovní spojení: Komerční banka
číslo účtu (CZK): [redacted]
IBAN: [redacted]
zastoupena: [redacted] místopředsedkyní představenstva
(dále jen „Dodavatel“)

u z a v í r a j í

tuto Smlouvu na rozvoj a údržbu DMS v letech 2021 - 2025 (dále jen „Smlouva“), v souladu s ustanoveními zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „zákon o veřejných zakázkách“), a v souladu s ustanovením § 1724 násl. zákona č. 89/2012 Sb., občanský zákoník (dále jen „občanský zákoník“).

1. DEFINICE POJMŮ

1.1. Nestanoví-li příslušné ustanovení této Smlouvy výslovně jinak, přikládají smluvní strany pojmům, použitým v této Smlouvě, dále uvedený obsah.

1.2. Smlouva: Smlouva na rozvoj a údržbu DMS v letech 2021 - 2025.

1.3. Standardy: Standardy otevřeného programování, veřejné standardy vydávané organizacemi ISO, IEEE, IETF, standardy vztahující se ke zvoleným technickým prostředkům.

1.4. Obecně závazné právní předpisy: Relevantní právní předpisy zejména zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů, zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů.

1.5. VZ, Veřejná zakázka: Veřejná zakázka „Rozvoj a údržbu DMS v letech 2021 - 2025“, Evid. číslo ve Věstníku veřejných zakázek: Z2021-008447, pro jejíž realizaci je tato Smlouva uzavírána.

1.6. ZD: Zadávací dokumentace VZ.

1.7. Součástí definic pojmů jsou i pojmy uvedené v Příloze č. 1 Smlouvy – Seznam použitých pojmů a zkratek.

2. ÚČEL A PŘEDMĚT SMLOUVY – PŘEDMĚT PLNĚNÍ VEŘEJNÉ ZAKÁZKY

2.1. Smluvní strany uzavírají tuto Smlouvu na rozvoj a údržbu aplikačního programového vybavení Document management system v letech 2021 – 2025 (dále též „Smlouva“) tak, aby jej mohl Zadavatel bezproblémově a v souladu s vývojem legislativy a dalších předpisů využívat pro výkon státní správy v oblasti centrálního ukládání a poskytování dat rezortu.

2.2. Smluvní strany prohlašují, že veškeré identifikační údaje uvedené v této Smlouvě jsou v souladu se skutečným stavem platným ke dni uzavření této Smlouvy.

2.3. Obsahem tohoto závazkového vztahu jsou všechny podmínky, práva a povinnosti stanovené v ZD, jejích přílohách a nabídce Dodavatele i v případě, že nejsou v této Smlouvě výslovně uvedeny. Smluvní strany prohlašují, že tuto Smlouvu, jakož i jednotlivá práva a povinnosti z ní vyplývající, budou vykládat v souladu se ZD, všemi podmínkami stanovenými v rámci zadávacího řízení na zadání Veřejné zakázky a nabídkou Dodavatele, předloženou v rámci zadávacího řízení, které předcházelo podpisu této Smlouvy.

2.4. Dodavatel prohlašuje, že je odborně způsobilý ke splnění všech svých závazků podle této Smlouvy, že se detailně seznámil s rozsahem a povahou Veřejné zakázky, že jsou mu známy veškeré technické, kvalitativní a jiné podmínky nezbytné k realizaci Veřejné zakázky a že disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci Veřejné zakázky za dohodnutou maximální smluvní cenu uvedenou v této Smlouvě, a to rovněž ve vazbě na jím prokázanou kvalifikaci pro plnění této Smlouvy.

2.5. Předmět této Smlouvy je definován následujícími základními celky:

2.5.1. Průběžný rozvoj, bezpečnost a údržba DMS

- Podrobný popis způsobu poskytování průběžného rozvoje, bezpečnosti a údržby DMS je uveden v Příloze 3 této Smlouvy.

2.5.2. Rozvoj a údržba DMS na objednávku

- Další požadavky, neřešené v rámci paušálního poplatku, budou řešeny na základě písemné objednávky Zadavatele.
- Celková pracnost rozvoje a údržby DMS nad rámec paušálu může za dobu účinnosti Smlouvy činit 800 ČLD s tím, že v tomto objemu pracnosti jsou zahrnuty i další činnosti, které bude Zadavatel požadovat řešit na základě objednávky.

- Rozvoj a údržba DMS na objednávku zahrnuje zejména:
    - rozvoj DMS nad rámec vyhrazených 10 ČLD měsíčně;
    - údržbu DMS nad rámec vyhrazených 10 ČLD měsíčně;
    - bezpečnost a aktualizaci bezpečnostní dokumentace nad rámec vyhrazených 2 ČLD měsíčně;
    - podporu při řešení havárií DMS (např. havárie na infrastruktuře);
    - řešení chyb ostatních komponent DMS, včetně SW;
    - podporu provozu DMS, např. monitorování provozu nad rámec uvedený v této Smlouvě, případně podpora při instalacích;
    - podporu nekomerčních (Open Source apod.) a ostatních software, pokud budou použity v DMS;
    - součinnost při řízení životního cyklu SW;
    - vypracování závazných technických podmínek pro obstarání TI;
    - mimořádné konzultace mimo běžný rámec podpory provozu a mimo řešení rozvojových požadavků, které jsou zpracovávány do konkrétních verzí DMS;
    - prezentace změn obsažených v aktuální dodávce;
    - školení.
- Služby spadající do služeb na objednávku mohou být provedeny pouze na základě předchozí objednávky Zadavatele a budou fakturovány na základě výkazů práce odsouhlasených a potvrzených Zadavatelem.

2.5.3. Aktualizace a vytvoření dokumentace pro zajištění bezpečnosti informací

2.6. Dodavatel se zavazuje provést řádně a včas plnění, které je předmětem této Smlouvy.

2.7. Zadavatel se zavazuje poskytnout Dodavateli nezbytnou součinnost způsobem stanoveným touto Smlouvou a zaplatit cenu, stanovenou na základě této Smlouvy.

2.8. Vymezení předmětu plnění této Smlouvy je podrobně uvedeno také v přílohách této Smlouvy.

3. DOBA PLNĚNÍ SMLOUVY

3.1. Smlouva je uzavřena na dobu určitou v délce trvání 48 měsíců od prvního dne měsíce následujícího po účinnosti smlouvy, nejdříve však od 1. 6. 2021.

4. MÍSTO PLNĚNÍ SMLOUVY

4.1. Místem plnění veřejné zakázky je především sídlo Zadavatele. Místem plnění veřejné zakázky je i housingové centrum T-Mobile v Praze, kde je umístěna část technického zařízení Zadavatele. Dojde-li ke změně housingového centra, zavazuje se Dodavatel tuto změnu respektovat. Místem plnění veřejné zakázky mohou být výjimečně také sídla katastrálních úřadů, katastrálních pracovišť, zeměměřických a katastrálních inspektorátů a Zeměměřického úřadu v celé ČR, pokud si to implementace některých budoucích funkcionalit vyžádá.

4.2. Místem plnění etap, jejichž výsledky budou pouze výstupní dokumenty a aplikační programové vybavení k testování, je sídlo Zadavatele.

4.3. Dodavatel zajistí, že jeho pracovníci podílející se na plnění této Smlouvy budou při pobytu na místech plnění uvedených výše dodržovat vnitřní předpisy Zadavatele, pokyny a směrnice upravující pohyb na pracovištích Zadavatele, požární bezpečnost, ochranu zdraví při práci a další předpisy, se kterými budou Zadavatelem seznámeni, přičemž o takovém seznámení musí být pořízen písemný zápis.

5. PERSONÁLNÍ ZAJIŠTĚNÍ SMLOUVY

5.1. Pro realizaci předmětu plnění této Smlouvy má Dodavatel připraven realizační tým specialistů, jehož klíčové osoby jsou uvedeny v Příloze 2 Smlouvy, kde jsou uvedeny i hlavní osoby Zadavatele, podílející se na součinnosti Zadavatele při plnění této Smlouvy.

5.2. Dodavatel deklaruje, že osoby, jejichž odbornou kvalifikací bylo prokázáno v nabídce Dodavatelem na plnění veřejné zakázky splnění kvalifikačních předpokladů nebo které byly Dodavatelem nabídnuty v rámci hodnocení jeho nabídky, budou skutečně zapojeny v dostatečném rozsahu dle povahy aktuálně poskytovaného plnění v uvedených rolích do plnění předmětu Smlouvy. Dodavatel je na vyžádání povinen kdykoliv skutečné zapojení těchto osob prokazatelně doložit. V případě nutné personální změny z důvodů mimo vůli Dodavatele v pozicích osob, jejichž odbornou kvalifikací bylo prokázáno splnění kvalifikačních předpokladů, musí Dodavatel doložit splnění srovnatelných kvalifikačních předpokladů pro osoby, jimiž budou uvolněné pozice obsazeny. Zadavatel si vyhrazuje právo na odmítnutí změn ve složení týmu Dodavatele v době plnění této Smlouvy, současně ale prohlašuje, že v případě potřeby změny bezdůvodně neodmítne. Po dobu, kdy Dodavatel neplní tento svůj závazek, je v prodlení s plněním dle této Smlouvy.

5.3. Pro realizaci předmětu plnění má Dodavatel právo použít smluvní poddodavatele. Seznam poddodavatelů předložil Dodavatel před podpisem této Smlouvy. Dodavatel má právo použít k plnění i další poddodavatele po předchozím písemném odsouhlasení Zadavatelem. Zadavatel odsouhlasení nového poddodavatele bezdůvodně neodmítne. Za plnění poddodavatelů odpovídá Dodavatel, jako by plnil sám.

5.4. Dodavatel deklaruje, že poddodavatelé, jejichž odbornou kvalifikací bylo prokázáno v nabídce Dodavatele na Veřejnou zakázku splnění kvalifikačních předpokladů, budou skutečně zapojeni do plnění předmětu Smlouvy minimálně v uvedeném rozsahu. V případě nutné změny takových poddodavatelů z důvodů mimo vůli Dodavatel musí Dodavatel doložit splnění srovnatelných kvalifikačních předpokladů pro nové poddodavatele. Zadavatel si vyhrazuje právo na odmítnutí změn poddodavatelů v době plnění této Smlouvy, současně ale prohlašuje, že v případě potřeby změny bezdůvodně neodmítne. Po dobu, kdy Dodavatel neplní tento svůj závazek, je v prodlení s plněním dle této Smlouvy.

6. TECHNOLOGICKÁ INFRASTRUKTURA A VÝVOJOVÉ PROSTŘEDÍ DODAVATELE

6.1. Pro realizaci předmětu této Smlouvy se Dodavatel zavazuje mít k dispozici technologickou infrastrukturu (dále jen „TI“) skládající se minimálně ze dvou samostatných prostředí, které využívají stejnou aplikační technologii a verze jako technologická infrastruktura Zadavatele. Dodavatel se dále zavazuje, že bude po celou dobu trvání Smlouvy umožňovat současný paralelní provoz minimálně jedné instance každého z následujících prostředí:

6.1.1. vývojového prostředí,

6.1.2. testovacího prostředí,

Testovací prostředí by mělo zajišťovat i testování napojení externích systémů pro dodavatele těchto externích systémů. Pokud nebude technologicky či organizačně možné takové prostředí pro dodavatele externích systémů připravit, je možné tento požadavek výjimečně, po předchozím výslovném písemném souhlasu Zadavatele, nahradit simulovaným prostředím, např. s využitím FAKE komponent.

6.2. Dodavatel zaručuje, že bude mít k dispozici TI potřebnou pro realizaci předmětu plnění této Smlouvy, a dále, že při návrzích na upgrade TI Zadavatele se bude řídit jen potřebami DMS bez ohledu na jím vlastněnou TI a jiné projekty. TI Dodavatele musí být plně zprovozněna a připravena k použití nejpozději do 3 měsíců od účinnosti Smlouvy.

6.3. Výchozí úroveň TI Dodavatele musí odpovídat popisu dle Přílohy ZD 3, s tím, že min. musí být shodný operační systém a verze produktů Oracle s provozní TI, včetně patchů a hotfixů, po celou dobu plnění Smlouvy. Dodavatel musí zajistit, aby při přenosu řešení z jeho referenční TI na TI provozovanou Zadavatelem:

6.3.1. nebyly vyvolávány/vytvářeny žádné dodatečné náklady na straně Zadavatele,

6.3.2. nebyly nutné na straně Zadavatele žádné speciální činnosti (kompilace modulů apod.),

6.3.3. bylo zajištěno stejné chování a funkce aplikace u Zadavatele, jako bylo u Dodavatele;

6.3.4. nevznikly jiné problémy způsobené případnou rozdílnou architekturou, např.:

6.3.4.1. jiné chování nebo činnosti databáze nebo aplikačního serveru;

6.3.4.2. nemožnost reprodukovat problém/chybu na straně Dodavatele;

6.3.4.3. problémy s platformově závislými chybami;

6.3.4.4. výkonnostní problémy, způsobené odladěním aplikace pouze pro TI Dodavatele.

7. METODIKA VÝVOJE, SOULAD SE STANDARDY

7.1. Při realizaci předmětu plnění této Smlouvy použije Dodavatel vlastní metodiku řízení projektu a vývoje IS. Dodavatel garantuje stálý soulad se všemi relevantními standardy, a to zejména se standardy otevřeného programování, s veřejnými standardy vydávanými organizacemi ISO, IEEE, IETF, se standardy vztahujícími se ke zvoleným technickým prostředkům, s prováděcí vyhláškou k ZoISVS, a to ve všech fázích a jednotlivých dílčích krocích při rozvoji DMS.

7.2. Podrobný popis metodiky vývoje je uveden v Příloze 6 Smlouvy.

7.3. Dodavatel s každou novou verzí DMS předá Zadavateli v elektronické podobě odpovídající uživatelské příručky / technologické postupy / popisy WS pro uživatele.

7.4. Zadavatel poskytne Dodavateli aktuální verze relevantní uživatelské dokumentace do 10 dnů od účinnosti Smlouvy.

8. ZAJIŠTĚNÍ KVALITY DODÁVEK DMS, INTERNÍ TESTOVÁNÍ

8.1. Dodavatel zajistí a garantuje pro systém DMS modifikovaný v rámci plnění této VZ, jeho funkčnost, výkonnost a UX alespoň na stávající úrovni (např. odezvy systému, jak u interaktivní práce uživatelů, tak u dávkových úloh, v relacích odpovídajících reálnému stavu při převzetí DMS), Dodavatel zajistí a garantuje nepřerušenou provozuschopnost DMS s výjimkou plánovaných odstávek.

8.2. Dodavatel se zavazuje ověřit kvalitu dodávek DMS před jejich předáním z hlediska souladu postupů s metodikou, standardy, obecně závaznými právními předpisy, apod. a též provedením interního testování, a to nejméně v tomto rozsahu:

8.2.1. testování funkcionality nových a měněných modulů;

8.2.2. ověření funkčnosti komunikace s externími informačními systémy;

8.2.3. provedení průřezových testů;

8.2.4. ověření instalace včetně kontroly správnosti a úplnosti sestavení dodávky;

8.2.5. ověření bezpečnosti webových služeb a aplikací;

8.2.6. ověření, zda výstup vyhovuje z hlediska výkonnosti a dostatečných odezev systému.

8.3. Součástí každé dodávky musí být kopie interních testovacích protokolů Dodavatele minimálně z výše uvedených interních testů provedených Dodavatelem. Pouze v případě předchozí písemné dohody (například zápisem z jednání projektového týmu) může být předání kopií interních testovacích protokolů Dodavatele výjimečně nahrazeno pouze písemným shrnutím výsledků interních testů Dodavatele.

8.4. Dodavatel se zavazuje provádět interní testování na vlastním testovacím prostředí. Před nasazením nové verze DMS do provozního prostředí musí být provedeny uživatelské, bezpečnostní a zátěžové testy, s tím, že nalezené kritické zranitelnosti v oblasti bezpečnosti musí být napraveny a opakovaně ověřeny před nasazením dané úpravy / dodávky do provozního prostředí. Závady zjištěné při zátěžových testech bude Dodavatel řešit v první řadě laděním / optimalizací aplikace.

8.5. Dodavatel se zavazuje, že:

8.5.1. dodá prohlášení / protokol o provedení interního testování a jeho výsledky (v elektronické podobě), a to jako součást předání každého výstupu k testování na referenčním prostředí Zadavatele, přičemž struktura, forma, věcný rozsah a způsob evidence v projektové kanceláři na straně Dodavatele budou upřesněny v součinnosti se Zadavatelem;

8.5.2. dodá testovací scénáře pro testování výstupu na straně Zadavatele, a to pro funkční / výkonnostní / akceptační testy;

8.5.3. po dodání výstupu a po jeho instalaci na referenční prostředí Zadavatele provede integrační testy (pokud jsou nutné), vybrané průřezové testy a výkonnostní testy, které zaručí, že je možné zahájit funkční / akceptační testování prováděné Zadavatelem;

8.5.4. všechny chyby, odhalené testováním, budou dokumentovány a klasifikovány podle jejich závažnosti;

8.5.5. všechny opravy chyb, zjištěných během testování, budou jednoznačným a pro Zadavatele dostupným způsobem evidovány a dokumentovány Dodavatelem;

8.5.6. všechny přechodové stavy v testovacích cyklech budou dokumentovány Dodavatelem;

8.5.7. osoby Dodavatele provádějící testování se nebudou podílet na vývoji oblastí, které testují;

8.5.8. umožní Zadavateli ověřit řešení / modifikaci pilotním provozem na vybraných úřadech či si k akceptačnímu řízení a k akceptačnímu testování přizvat externího konzultanta.

8.6. Dodavatel je povinen prokazatelným způsobem evidovat počet zjištěných chyb (např. ve formě samostatné položky v HD Dodavatele) tak, aby smluvní strany na tomto základě mohly výskyt chyb průběžně sledovat.

9. POVINNOSTI DODAVATELE

9.1. Dodavatel deklaruje, že předmět plnění podle Smlouvy není plněním nemožným a že tuto Smlouvu uzavírá po pečlivém zvážení všech možných důsledků. Dodavatel dále prohlašuje, že se seznámil s předmětem této Smlouvy, a že dílo může být dokončeno způsobem a v termínech stanovených v této Smlouvě.

9.2. Dodavatel se zavazuje, že pokud budou v rámci plnění této Smlouvy dodány licence SW nad rámec stávajícího stavu, zajistí licenční soulad s pravidly konkrétního výrobce, a to na vlastní náklady.

9.3. Dodavatel se zavazuje, že pro plnění na objednávku bude Zadavateli předkládat v termínech dle harmonogramu daného plnění k odsouhlasení návrhy pracnosti analýz jednotlivých modifikací požadovaných Zadavatelem k řešení. Práce Dodavatele na analýze, jejíž pracnost nebyla Zadavatelem předem odsouhlasena, nebude Dodavateli uhrazena. Součástí analýzy bude i (případně variantní) návrh celkové pracnosti realizace.

9.4. Dodavatel se zavazuje, že pro plnění na objednávku bude Zadavateli předkládat k odsouhlasení návrhy celkové pracnosti implementace změny, s tím, že u změny/modifikace přesahující pracnost implementace 30 člověkodní, Dodavatel doloží podrobně pracnost pro:

- design;
- programátorské činnosti (po modulech / komponentách);
- testování;
- napojení na systémy třetích stran pro účely integrace / testování;
- činnosti spojené s instalací řešení do provozu;
- činnosti spojené s monitorováním po instalaci daného řešení do provozu (pro následné předání Zadavateli, včetně dokumentace).

9.5. Při plnění předmětu této Smlouvy se Dodavatel zavazuje dodržovat všechny relevantní právní předpisy, opatření a pokyny, upravující působnost a činnost Zadavatele. Při plnění předmětu této Smlouvy se Dodavatel zavazuje dodržovat také všechny relevantní platné právní předpisy, normy obsahující technické specifikace a technická řešení, technické a technologické postupy nebo jiná určující kritéria pro předmět plnění. Výsledek předmětu plnění musí být v souladu s normou ČSN EN ISO 90001:2001 Systémy managementu jakosti.

9.6. Při plnění předmětu této Smlouvy se Dodavatel zavazuje udržovat následující výstupy v aktuálním stavu a na vyžádání je ve lhůtě 1 měsíce Zadavateli předávat, s tím, že poslední předání výstupů Zadavateli bude k datu ukončení smluvního vztahu, jedná se zejména o:

- popis používaných nástrojů a jejich nastavení,
- popis konfiguračního řízení,
- projektové standardy (jmenné konvence apod.),
- použité způsoby a metodiky vývoje,
- principy monitorování a aktualizace požadavků v systému pro evidenci požadavků,
- popis monitorování provozu,
- bezpečnostní dokumentaci,
- obsah projektové kanceláře, a to ve formě umožňující off-line procházení a čtení veškeré dokumentace vložené do PK, včetně všech verzí,
- export problémů / požadavků z HD Dodavatele.

9.7. Zadavatel v souladu s ustanovením § 6 odst. 4 zákona o zdávání veřejných zakázek trvá na dodržování zásady sociálně odpovědného zadávání, environmentálně odpovědného zadávání a inovací. S ohledem na charakter zakázky Zadavatel zejména požaduje po Dodavateli, aby v průběhu plnění této Smlouvy dodržoval a zajistil dodržování pracovněprávních předpisů (zejména zákoníku práce a zákona o zaměstnanosti) vůči všem osobám, které se na plnění této Smlouvy budou podílet. Dodavatel se zavazuje, že bude dodržovat veškerá ustanovení pracovněprávních předpisů, zejména zákoník práce a zákon o zaměstnanosti, a v případě požadavku Zadavatele mu dodržování daných povinností doloží.

10. ZABEZPEČENÍ OCHRANY DAT DMS PŘED ZNEUŽITÍM, OCHRANA ÚDAJŮ

10.1. Při realizaci předmětu Smlouvy Dodavatel garantuje zachování bezpečnosti DMS alespoň na dosavadní úrovni.

10.2. Dodavatel se zavazuje pro případ, že se v průběhu plnění předmětu Smlouvy dostane do kontaktu s údaji Zadavatele vyplývajícími z jeho provozní činnosti, tyto údaje v žádném případě nezneužít, nezveřejnit, nepředat třetí osobě, nezměnit, ani jinak nepoškodit, ztratit či znehodnotit.

10.3. Dodavatel se rovněž zavazuje provádět svoje činnosti tak, aby nebyla v nadbytečném rozsahu omezena činnost uživatelů DMS, zejména v úředních hodinách.

10.4. Při realizaci předmětu Smlouvy Dodavatel garantuje odstranění zranitelností webových aplikací a služeb zjištěných externími penetračními testy, jako vady.

11. SOUČINNOST ZADAVATELE A DODAVATELE, STANOVENÍ ŘÍDÍCÍCH A VÝKONNÝCH ORGÁNŮ PROJEKTU, ŘÍZENÍ A KOMUNIKACE NA PROJEKTU

11.1. Smluvní strany se zavazují úzce spolupracovat, zejména si poskytovat úplné, pravdivé a včasné informace potřebné k řádnému plnění svých závazků, přičemž v případě změny podstatných okolností, které mají nebo mohou mít vliv na plnění této Smlouvy, jsou povinny o takové změně informovat druhou smluvní stranu nejpozději do tří (3) pracovních dnů po vzniku takové změny.

11.2. Zadavatel se zavazuje poskytnout Dodavateli nezbytnou součinnost způsobem stanoveným touto Smlouvou. Součinnost, kterou je dle této Smlouvy povinen Zadavatel poskytnout Dodavateli, se Zadavatel zavazuje poskytnout i poddodavatelům Dodavatele, které Dodavatel v souladu s touto Smlouvou použije při plnění dle této Smlouvy. Zadavatel je povinen poskytnout součinnost definovanou v této Smlouvě, a dále součinnost, kterou písemně dohodnou oprávněné osoby.

11.3. Smluvní strany se dále zavazují vytvořit druhé smluvní straně dohodnuté podmínky, umožňující řádné plnění této Smlouvy.

11.4. V zájmu optimálního plnění této Smlouvy jsou smluvní strany povinny plnit řádně a včas své závazky tak, aby nedocházelo k prodlení s jejich plněním. Pokud se některá ze smluvních stran dostane do prodlení s plněním svých závazků, je povinna oznámit bez zbytečného odkladu druhé smluvní straně důvod prodlení a předpokládaný termín a způsob jeho odstranění.

11.5. Smluvní strany se zavazují plnit své závazky v souladu se všemi příslušnými právními předpisy.

11.6. Dodavatel se zavazuje poskytovat Zadavateli součinnost při přebírání, akceptaci a atestaci výstupů v rozsahu stanoveném touto Smlouvou.

11.7. Žádná ze smluvních stran není odpovědna za prodlení způsobené prodlením s plněním závazků druhé smluvní strany.

11.8. Požadavky na způsob řízení projektu, včetně obsazení základních rolí, jsou uvedeny v Příloze 2 Smlouvy. Personální změny osob každé ze smluvních stran podléhají písemnému oznámení druhé smluvní straně, aniž by smluvní strany byly povinny uzavírat dodatek této Smlouvy. Povinnosti Dodavatele ve smyslu čl. 5.2. tím nejsou dotčeny.

11.9. Komunikace smluvních stran probíhá na úrovni oprávněných osob a jejich zástupců, definovaných v čl. 14.4. Zástupci oprávněných osob přitom oprávněnou osobu zastupují při plnění její působnosti. Tím není dotčena možnost smluvních stran komunikovat prostřednictvím statutárních orgánů.

11.10. Součinnost smluvních stran při plnění této Smlouvy v oblasti evidence požadavků na úpravy DMS bude též realizována prostřednictvím Service Desk Manageru Zadavatele (dále též „SDM“), provozovaném na produktu CA Service Desk Manager verze r.12.9., a HelpDesku Dodavatele, s tím, že podrobnosti jsou uvedeny v Příloze 4 Smlouvy.

12. VYPRACOVÁNÍ PODKLADŮ PRO PŘÍPADNÉ OBSTARÁNÍ TECHNOLOGICKÉ INFRASTRUKTURY

12.1. Vypracování podkladů pro případné obstarání technologické infrastruktury by byly dohodnuty v objednávce.

13. PŘEBÍRÁNÍ VÝSTUPŮ, AKCEPTAČNÍ ŘÍZENÍ

13.1. Výstupy každé jednotlivé etapy projektu předá Dodavatel Zadavateli ve stanovených termínech. O předání a převzetí těchto výstupů bude sepsán předávací protokol podepsaný oprávněnými osobami obou smluvních stran.

13.2. Akceptační řízení začne nejpozději jedenáctý pracovní den po předání plnění, pokud při převzetí plnění nedojde k jiné dohodě. Zadavatel vyvolá oponentní řízení převzatého plnění nejméně dva pracovní dny před akceptačním řízením, které se koná ve smluvně dohodnutém termínu, a sdělí Dodavateli výhrady k předanému plnění s vyznačením jejich závažností. V rámci akceptačního řízení budou projednány výhrady Zadavatele, stanovena jejich výsledná závažnost a určen způsob a termín jejich odstranění. Při stanovení výsledné závažnosti připomínek Zadavatel vezme do úvahy stanovisko Dodavatele. Akceptační řízení musí být ukončeno nejpozději patnáctý pracovní den po jeho zahájení.

13.3. Akceptační řízení musí vést k některému z těchto tří závěrů:

13.3.1. **Akceptováno bez výhrad**. V případě, že Zadavatel v průběhu akceptačního řízení nenalezne v předaném plnění žádné vady ani nedodělky, uvede Zadavatel do akceptačního protokolu, že předané plnění bylo akceptováno bez výhrad a akceptační protokol potvrdí svým podpisem.

13.3.2. **Akceptováno s výhradami**. V případě, že budou v průběhu akceptačního řízení zjištěny v předaném plnění vady nebo nedodělky, nebránící dalšímu užití díla, dohodnou se Zadavatel a Dodavatel na termínu, do kterého Dodavatel zjištěné vady a nedodělky odstraní/dořeší. Zadavatel do akceptačního protokolu uvede seznam vad nebo nedodělků s termíny jejich odstranění. V akceptačním protokolu se uvede, že předané plnění bylo akceptováno s uvedenými výhradami a obě strany akceptační protokol potvrdí svým podpisem. Další postup dle článku 13.4. V případě, že Dodavatel neodstraní/nedořeší vady a nedodělky ve stanoveném termínu, bude Zadavatel požadovat slevu z ceny plnění, viz ustanovení níže.

13.3.3. **Neakceptováno**. V případě, že budou v průběhu akceptačního řízení v předaném plnění zjištěny takové vady a nedodělky, které by bránily v užití díla či jeho části, není předané plnění akceptováno. Obě strany se dohodnou na termínech nového předání a nového akceptačního řízení. Do akceptačního protokolu Zadavatel uvede, že předané plnění nebylo akceptováno, dohodnuté termíny nového předání a akceptačního řízení a obě strany akceptační protokol potvrdí svým podpisem; od tohoto okamžiku se počítá (případně pokračuje v přičítání) výše sankce za prodlení s plněním.

13.4. Pokud je akceptační řízení ukončeno s výsledkem „Akceptováno s výhradami“, bude stanoveno zádržné jako část z ceny daného dílčího plnění, které bude vázáno na vyřešení všech výhrad z akceptace dle odsouhlasených postupů a termínů (dále jen „Doplatek“). Maximální možná výše Doplatku je 50 % ceny dílčího plnění. Dodavatel je v případě akceptace s výhradami oprávněn fakturovat takto:

13.4.1. po podpisu akceptačního protokolu částku ve výši ceny dílčího plnění poníženou o Doplatek.

13.4.2. Po podpisu protokolu o vyřešení všech výhrad z akceptace dle odsouhlasených postupů a termínů je Dodavatel oprávněn fakturovat částku dle Doplatku, případně poníženou o slevu z ceny pro případy, že výhrady byly vyřešeny po termíny stanoveném k jejich odstranění/vyřešení a zároveň poníženou o 10 % z výše Doplatku, a to za každý i započatý měsíc od data, ke kterému mělo být akceptační řízení ukončeno dle čl. 13.1 a 13.2 Smlouvy. Měsícem se přitom rozumí 30 kalendářních dní. Minimální snížení Doplatku přitom činí 10 % z výše Doplatku..

13.4.3. Obě strany se mohou v rámci akceptačního řízení písemně dohodnout na tom, že výhrady z akceptace budou vyřešeny ve více krocích, zpravidla vázaných k dalším dodávkám DMS. Doplatek pak bude fakturován ve více dílčích částkách odpovídajících vyřešené části výhrad z akceptace v daném kroku na základě podpisu protokolu o vyřešení výhrad z akceptace příslušných danému kroku; přitom se pro případné ponížení Doplatku použije postup dle bodu 13.4.2

13.5. Dodavatel před instalací každé nové verze DMS do prvního referenčního prostředí (DMS DEV nebo DMS TEST) předá Zadavateli:

13.5.1. výstupní protokol z interního testování na straně Dodavatele,

13.5.2. testovací scénáře ve formátu DOC (DOCX) a XLS (XLSX), který umožňuje import do SpiraTest (import do SpiraTest probíhá pomocí doplňku MS Office SpiraExcelAddIn),

13.5.3. všechny zdrojové kódy včetně použitých nekomerčních (Open Source) SW, přičemž dokumentace zdrojových kódů musí být na takové úrovni, aby byla srozumitelná i třetí, nezúčastněné osobě,

13.5.4. uživatelská příručka,

13.5.5. instalační příručka,

13.5.6. dokumentace webových služeb a dokumentaci všech WSDL, XML, XSD včetně podrobných komentářů jednotlivých elementů a atributů,

13.5.7. provozní dokumentace,

13.5.8. dokumentace pro školení.

13.6. Dodavatel po instalaci každé nové verze DMS do produkčního prostředí dle této Smlouvy předá Zadavateli zejména následující finalizované výstupy z plnění potřebné pro další rozvoj a údržbu DMS:

13.6.1. všechny zdrojové kódy včetně použitých nekomerčních (Open Source) SW, přičemž dokumentace zdrojových kódů musí být na takové úrovni, aby byla srozumitelná i třetí, nezúčastněné osobě,

13.6.2. exporty repository všech použitých nástrojů, pomocných skriptů, utilit (např. pro konfigurační řízení apod.),

13.6.3. analytické modely – procesní analýza (business model i model firemních procesů), globální specifikace systému v UML min. v rozsahu identifikace a modelování typových úloh se specifikací uživatelských požadavků, identifikaci aktérů v příslušných diagramech, datový model, (business i prezentační vrstva), model požadavků, implementační model (s důrazem na implementaci komponent), model návrhu,

13.6.4. programátorská dokumentace,

13.6.5. uživatelská příručka,

13.6.6. instalační příručka,

13.6.7. dokumentace webových služeb a dokumentaci všech WSDL, XML, XSD včetně podrobných komentářů jednotlivých elementů a atributů,

13.6.8. popis TI, včetně všech komponent, analytické dokumenty odpovídající reálnému nasazení systému do ostrého provozu, včetně všech jeho komponent,

13.6.9. výsledky bezpečnostních testů a provedení kontrolních checklistů,

13.6.10. dotčená (změněná) provozní dokumentace,

13.6.11. systémová příručka IS,

13.6.12. dokumentace pro školení.

14. POVĚŘENÍ ZAMĚSTNANCI ZADAVATELE A DODAVATELE

14.1. Pověření zaměstnanci smluvních stran jsou oprávněnými osobami podle této Smlouvy a jsou oprávněni zastupovat smluvní stranu při plnění této Smlouvy a při jednáních souvisejících s přípravou dílčích objednávek nebo dodatků Smlouvy. V případě změny oprávněné osoby nebo jejího zástupce je dotyčná strana povinna písemně informovat druhou smluvní stranu nejpozději pět dnů před provedením změny.

14.2. Všechny dokumenty, mající vztah k plnění této Smlouvy, musí být podepsány oprávněnými osobami obou smluvních stran nebo jejich zástupci.

14.3. Do působnosti oprávněných osob náleží:

14.3.1. kontrolovat postup plnění této Smlouvy;

14.3.2. připravovat návrhy potřebných změn a dodatků této Smlouvy a dílčích objednávek, připravovat návrhy dalších dílčích objednávek a předkládat takové návrhy smluvním stranám k uzavření;

14.3.3. organizačně zabezpečovat veškeré činnosti související s plněním této Smlouvy;

14.3.4. koordinovat součinnost smluvních stran;

14.3.5. informovat na vyžádání smluvní strany o postupu plnění této Smlouvy.

14.4. Objednávka Zadavatele musí být podepsaná oprávněnou osobou Zadavatele a potvrzená oprávněnou osobou Dodavatele (viz kapitola 14.6).

14.5. Měsíční výkazy práce a akceptace objednávek musí být odsouhlaseny a potvrzeny podpisem oprávněné osoby Zadavatele i Dodavatele, případně jejich zástupců (viz kapitola 14.6).

14.6. Oprávněnými osobami jsou:

	Zadavatel	Dodavatel
Oprávněné osoby	[redacted]	[redacted]
Zástupci oprávněných osob	[redacted] – ředitelka projektu [redacted] - vedoucí projektu	[redacted] – vedoucí projektu

15. CENA PLNĚNÍ

15.1. Celková cena plnění podle této Smlouvy činí 42 450 000 Kč bez DPH. Uvedená celková cena představuje cenu maximální, které je možno dosáhnout za všechna plnění podle této Smlouvy, včetně plnění na základě objednávek, nezakládá však nárok Dodavatele na proplacení celé uvedené ceny Zadavatelem. Celková cena bude uhrazována v průběhu plnění této Smlouvy za jednotlivá plnění podle Smlouvy.

15.2. Jednotkové ceny resp. jednotlivé položky činí:

Položka	Plnění	Jednotka	Počet jednotek	Celková cena v Kč bez DPH
1	Rozvoj a údržba na objednávku	1 ČLD	800	6 480 000
2	Průběžný rozvoj, bezpečnost a údržba	1 kalendářní měsíc	48	35 520 000
3	Bezpečnostní dokumentace	Celé plnění	1	450 000
	CELKEM			42 450 000

15.3. Celková cena plnění je stanovena jako nejvýše přípustná a nepřekročitelná a zahrnující veškeré náklady Dodavatele včetně nákladů spojených s dopravou do míst plnění této Smlouvy, pojištěním, nákladů spojených s telefonickými hovory, nocležným atd. Dodavatel deklaruje, že je schopen za tuto cenu splnit požadavky uvedené v předmětu této Smlouvy.

15.4. Při fakturaci bude k dohodnutým cenám připočtena DPH dle aktuálně platných právních předpisů.

16. PLATEBNÍ A FAKTURAČNÍ PODMÍNKY

16.1. Právo fakturovat vzniká Dodavateli vždy v návaznosti na oboustranně odsouhlasené a podepsané výstupy v rámci plnění.

16.2. Dodavatel je povinen, po vzniku práva fakturovat, vystavit a Zadavateli předat fakturu v elektronické podobě (datová schránka Zadavatele, email podatelny Zadavatele) nebo listinné podobě ve dvojím vyhotovení (osobně na podatelnu Zadavatele, nebo poštou na adresu Zadavatele). Zadavatel upřednostňuje elektronické podání.

16.3. Vyúčtování ceny za provedení plnění, provede Dodavatel na základě daňového dokladu – faktury, splňující veškeré podstatné náležitosti dle zvláštních právních předpisů, zejména zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů. V každé faktuře Dodavatele musí být odkaz na č. j. Smlouvy přidělené Zadavatelem a v případě, že se jedná o fakturu za Rozvoj a údržbu na objednávku i č.j. Objednávky přidělené Zadavatelem. Společně s fakturami Dodavatel poskytne kopie, či skeny následujících dokumentů. Pro fakturaci za Průběžný rozvoj, bezpečnost a údržbu musí být přílohou schválené všechny měsíční výkazy práce za dané fakturační čtvrtletí. Pro fakturaci za Rozvoj a údržbu na objednávku a za Bezpečnostní dokumentaci musí být přiložen schválený akceptační protokol

16.4. Pro jednotlivé části plnění ve smyslu odst. 15.2. jsou platné navíc tyto specifické platební podmínky:

16.4.1. Pro fakturaci cen podle odst. 15.2., položky 1 se za den uskutečnění zdanitelného plnění považuje den akceptace předmětu plnění (výstupu) Zadavatelem. Po tomto dni je Dodavatel oprávněn předložit Zadavateli fakturu. Součástí faktury formou přílohy bude protokol o předání a převzetí výstupu a jeho akceptaci Zadavatelem. V případě, že se strany dohodnou, lze časově delší plnění dle odst. 15.2., položky 1 akceptovat potvrzením měsíčního výkazu práce, přičemž fakturačním obdobím bude ukončené čtvrtletí v rámci plnění Smlouvy. Fakturu na úhradu prací na základě objednávky je Dodavatel oprávněn vystavit nejdříve první pracovní den po uplynutí fakturačního období. Součástí faktury formou přílohy bude výkaz práce včetně uvedení pracnosti jednotlivých činností v hodinách potvrzený Zadavatelem. Nejmenší jednotkou pro fakturaci je jedna hodina.

16.4.2. Pro fakturaci ceny podle odst. 15.2., položka 2 je fakturačním obdobím čtvrtletí poskytování plnění. Fakturu na úhradu ceny je Dodavatel oprávněn vystavit nejdříve první pracovní den po uplynutí fakturačního období. Součástí faktury budou formou přílohy výkazy či přehledy s výsledky průběžného rozvoje, bezpečnosti a údržby včetně dokumentace vyřešených oprav vad včetně uvedení pracnosti v ČLD v předmětném fakturačním období.

16.4.3. Fakturace ceny podle odst. 15.3., položka 3 bude provedena po akceptaci jednorázově.

16.5. Faktura je splatná do 21 kalendářních dnů ode dne jejího doručení Zadavateli. V případě předložení faktury v období od 15. prosince do 31. ledna bude splatnost faktury stanovena na 30 dnů ode dne doručení Zadavateli.

16.6. Zadavatel je oprávněn do data splatnosti vrátit fakturu, která neobsahuje požadované náležitosti, není doložena kopií potvrzeného akceptačního protokolu, a která obsahuje jiné cenové údaje nebo jiný druh plnění než dohodnuté v této Smlouvě nebo dílčí objednávce s tím, že doba splatnosti nové (opravené) faktury začíná znovu běžet ode dne jejího doručení Zadavateli.

16.7. Faktura je považována za proplacenou okamžikem odepsání příslušné částky z účtu Zadavatele ve prospěch Dodavatele.

16.8. Zadavatel neposkytuje zálohové platby.

17. PRÁVA A POVINNOSTI SMLUVNÍCH STRAN

17.1. Dodavatel je povinen provést plnění podle této Smlouvy a případných objednávek řádně a odevzdat plnění Zadavateli ve stanoveném termínu, na stanoveném místě a v dohodnuté kvalitě.

17.2. Dodavatel se zavazuje informovat Zadavatele o veškerých skutečnostech, které jsou nebo mohou být významné pro rozhodování Zadavatele týkající se předmětu plnění a upozornit ho na případnou nesprávnost rozhodnutí a opatření učiněných v souvislosti s jeho závazky podle této Smlouvy.

17.3. Zadavatel se zavazuje předat Dodavateli potřebné podklady dohodnuté oprávněnými osobami, a to v dohodnutých termínech, pokud to nevyloučí okolnosti způsobené třetí stranou mimo jeho působnost.

17.4. Zadavatel se zavazuje umožnit Dodavateli, resp. jeho pracovníkům vyčleněným pro plnění dle této Smlouvy, přístup na pracoviště Zadavatele a k programovému vybavení Zadavatele (mimo zdrojové texty) v rozsahu nezbytném pro řádné plnění této Smlouvy.

17.5. Dodavatel se zavazuje umožnit Zadavateli, resp. jeho pracovníkům, vyčleněným pro plnění dle této Smlouvy, přístup na pracoviště Dodavatele a k programovému vybavení Dodavatele (zejména k vývojovému prostředí, produktům, nástrojů, dokumentaci a dalším podkladům a výstupům souvisejícím s plněním) v rozsahu nezbytném pro řádné plnění této Smlouvy.

17.6. Smluvní strany se zavazují úzce spolupracovat při veřejné prezentaci projektu, ve vztahu k odborné veřejnosti a při popularizaci jeho výsledků.

17.7. Smluvní strany jsou povinny plnit své závazky vyplývající z této Smlouvy tak, aby nedocházelo k prodlení s plněním jednotlivých termínů a k prodlením s placením jednotlivých peněžních závazků.

17.8. Smluvní strany se zavazují plnit své závazky vyplývající z této Smlouvy tak, aby byly šetřeny oprávněné zájmy druhé smluvní strany a aby nedocházelo k nadbytečnému zvyšování nákladů druhé smluvní strany.

17.9. Pokud některá ze smluvních stran neplní povinnosti nebo nedodrží své závazky stanovené touto Smlouvou, nevzniká tím druhé straně právo, aby rovněž neplnila své povinnosti nebo nedodržela své závazky kromě případů, které jsou výslovně upraveny touto Smlouvou.

17.10. Smluvní strana je oprávněna požadovat od druhé smluvní strany řádné a včasné plnění včetně náhrady za způsobenou škodu.

17.11. Žádná ze smluvních stran není odpovědná za prodlení se splněním svých závazků, způsobené okolnostmi vylučujícími odpovědnost (vyšší mocí).

17.12. Smluvní strany se zavazují upozornit druhou smluvní stranu bez zbytečného odkladu na vzniklé okolnosti vylučující odpovědnost bránící řádnému plnění této Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání okolností vylučujících odpovědnost.

17.13. Všechny dokumenty mající vztah k plnění této Smlouvy, představující vícestranné či jednostranné úkony smluvních stran, například zápisy z jednání, dodatky k zadání, protokoly, výzvy, výpovědi, upozornění, žádosti a jiná oznámení, musí být podepsány oprávněnými osobami.

17.14. Dokumenty uvedené v předchozím odstavci se vždy doručují druhé smluvní straně, a to některým ze způsobů dále uvedených:

17.14.1. osobně oproti potvrzení o převzetí;

17.14.2. doporučeným dopisem či jinou formou registrovaného poštovního styku. V tomto případě se dokumenty považují za doručené dnem jejich převzetí adresátem, dnem vrácení zásilky v případě, že si ji adresát nevyzvedl, a dále dnem, kdy adresát převzetí zásilky odmítl;

17.14.3. elektronickou poštou. V tomto případě se dokumenty považují za doručené okamžikem, kdy odesílatel obdrží od příslušného technického zařízení potvrzení o úspěšném odeslání anebo potvrzení o doručení. Pro odstranění případných nedorozumění se smluvní strany zavazují vzájemně informovat o řádném doručení dokumentů zaslaných tímto způsobem;

17.14.4. do datové schránky příjemce.

17.15. V případě doručování dokumentů v elektronické podobě budou smluvní strany používat formát MS Office 2016 nebo vyšší, případně pdf, zip, rar. Dokumenty v elektronické podobě lze doručovat prostřednictvím elektronické pošty nebo na dohodnutém datovém médiu.

17.16. Dodavatel tímto dává souhlas se zveřejněním této Smlouvy v souladu s povinnostmi Zadavatele podle právních předpisů.

17.17. Dodavatel bude postupovat při plnění předmětu této Smlouvy s odbornou péčí, podle nejlepších znalostí a schopností, sledovat a chránit oprávněné zájmy Zadavatele a postupovat v souladu s jeho pokyny a interními předpisy souvisejícími s předmětem plnění této Smlouvy (či její dílčí části), které Zadavatel Dodavateli poskytne nebo s pokyny jím pověřených osob. Dodavatel rovněž poskytne Zadavateli veškerou nezbytnou součinnost k naplnění účelu Smlouvy.

17.18. Dodavatel se zavazuje respektovat pracovní dobu Zadavatele, a to zejména v případech, kdy je nezbytná součinnost pracovníků Zadavatele v rámci realizace úkolu Dodavatele. Případné lhůty stanovené pro součinnost Zadavatele běží pouze v příslušné pracovní době. Pro účely plnění dle této Smlouvy se za pracovní dobu na straně Zadavatele považuje v pracovních dnech:

17.18.1. pro operátory Helpdesku doba od 7:00 do 17:00 hodin;

17.18.2. pro testery a konzultanty doba od 7:00 do 15:00 hodin;

17.18.3. pro zástupce sekce centrální databáze doba od 8:00 do 17:00 hodin;

17.18.4. pro vedení projektu doba od 8:00 do 17:00 hodin.

17.19. Dodavatel se zavazuje udržovat v platnosti Smlouvu o pojištění odpovědnosti za škodu způsobenou Dodavatelem třetí osobě, přičemž limit pojistného plnění vyplývající z pojistné smlouvy nesmí být nižší než 100.000.000,- Kč. Takovou Smlouvu o pojištění odpovědnosti za škodu způsobenou Dodavatelem třetí osobě Dodavatel předloží Zadavateli na vyžádání. Dodavatel je dále povinen informovat Zadavatele o změnách v pojistné smlouvě a Zadavatel má právo požadovat předložení dodatků, případně nově uzavřené pojistné smlouvy.

17.20. Dodavatel se zavazuje udržovat v platnosti po celou dobu plnění závazků ze Smlouvy certifikáty a osvědčení stanovené v zadávací dokumentaci Veřejné zakázky, vztahující se k Zadavateli a osobám, které se budou podílet na provádění Smlouvy. Po dobu, kdy Dodavatel neplní tento svůj závazek, je v prodlení s plněním dle této Smlouvy.

17.21. Dodavatel souhlasí, aby subjekty, oprávněné dle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, provedly finanční kontrolu závazkového vztahu vyplývajícího ze Smlouvy s tím, že se Dodavatel podrobí této kontrole, a bude působit jako osoba povinná ve smyslu ustanovení § 2 písm. e) uvedeného zákona.

17.22. Dodavatel se zavazuje zachovávat mlčenlivost ohledně skutečností, které se v souvislosti s plněním této Smlouvy dozvěděl a které Zadavatel označil za důvěrné (dále jen „důvěrné informace“). Dodavatel je povinen přijmout opatření k ochraně důvěrných informací. Důvěrné informace mohou být Dodavatelem použity výhradně k činnostem, kterými bude zajištěno dosažení účelu této Smlouvy. Dodavatel nesdělí či nezpřístupní žádnou z důvěrných informací třetím osobám, nevyužije ji k vlastnímu prospěchu nebo jinak nezneužije. Povinnost mlčenlivosti a zachování důvěrnosti informací se nevztahuje na informace, které se staly obecně známými za předpokladu, že se tak nestalo porušením některé z povinností vyplývajících z této Smlouvy, nebo o kterých tak stanoví zákon, zpřístupnění je však možné vždy jen v nezbytném rozsahu a po předchozím písemném souhlasu Dodavatele.

17.23. Ujednání o ochraně důvěrných informací není dotčeno ukončením účinnosti této Smlouvy z jakéhokoliv důvodu a jeho účinnost skončí dva roky po skončení účinnosti této Smlouvy, nedohodnou-li se smluvní strany výslovně jinak.

17.24. Zadavatel je oprávněn v průběhu plnění této Smlouvy požadovat zprávy (reporty) o průběžném stavu plnění, včetně úplného exportu obsahu Projektové kanceláře.

18. ZÁRUKA, PODMÍNKY ZÁRUČNÍ PODPORY

18.1. Dodavatel garantuje, že DMS bude fungovat v souladu s touto Smlouvou a ZD. Dodavatel přebírá závazek odstranit na své náklady vady díla, jež bude mít dílo v době jeho předání Zadavateli, a dále odstranit na své náklady vady díla, které se vyskytnou v průběhu záruční doby.

18.2. Záruční doba, ve které bude Dodavatel odstraňovat vady plnění bezplatně, bude trvat dva roky od akceptace daného plnění, zároveň však nejdéle do konce této Smlouvy.

18.3. Záruka:

18.3.1. se vztahuje na všechny části díla, včetně příslušenství a případně využitého nekomerčního (Open Source) SW;

18.3.2. se vztahuje na funkčnost díla, jakož i na vlastnosti požadované Zadavatelem;

18.3.3. se prodlužuje o dobu, po kterou mělo dílo vadu bránící jeho řádnému užívání Zadavatelem;

18.4. Dodavatel odpovídá Zadavateli za případnou škodu, která mu vznikne z titulu neodstranění vady díla Dodavatelem ve sjednaném termínu.

18.5. Detailní popis záruky a podmínek záruční podpory je uveden v Příloze 3 Smlouvy.

18.6. Záruka bude ukončena dříve než před uplynutím dohodnuté záruční doby v okamžiku, kdy do DMS či jeho dílčí části, pro kterou je stanovena samostatná záruční doba, nepovoleně zasáhne (ve smyslu modifikace DMS, datové struktury či TI) třetí osoba nebo Zadavatel sám, není-li dále stanoveno jinak. Nepovoleným zásahem se nerozumí provozní zásahy Zadavatele podle dokumentace předané Dodavatelem a zásahy na základě schváleného změnového řízení.

18.7. V případě, že do DMS zasáhne třetí osoba, vybraná v zadávacím řízení, a bude prokázáno, že vada DMS je vadou, za kterou je odpovědný Dodavatel, neboť byla vadou DMS ještě před zásahem třetí osoby, poskytne v prvních 3 měsících po ukončení této Smlouvy Dodavatel zdarma třetí osobě vybrané v zadávacím řízení podporu za účelem odstranění vady. Vada musí být opakovatelná na poslední verzi DMS, kterou Dodavatel předal Zadavateli.

19. ODPOVĚDNOST SMLUVNÍCH STRAN ZA NEPLNĚNÍ PODMÍNEK SMLOUVY, ODPOVĚDNOST DODAVATELE ZA ŠKODU, VADY A SANKCE

19.1. Smluvní strany nesou odpovědnost za způsobenou škodu v rámci platných a účinných právních předpisů a Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.

19.2. Žádná ze smluvních stran neodpovídá za škodu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé smluvní strany. Dodavatel je však povinen upozornit bez prodlení Zadavatele, jakmile zjistí, že zadání je věcně nesprávné nebo chybné a nepokračovat v řešení do projednání se Zadavatelem a upřesnění zadání. V takovém případě není Dodavatel do upřesnění zadání ze strany Zadavatele v prodlení s plněním, s nímž věcně nesprávné nebo chybné zadání Zadavatele souvisí. Dodavatel je rovněž povinen aktivně hledat optimální řešení a upozornit Zadavatele, pokud shledá, že zadaného cíle je možno dosáhnout výhodnějším způsobem než podle zadání Zadavatele.

19.3. Nahrazuje se pouze skutečně vzniklá škoda v souladu s příslušnými ustanoveními občanského zákoníku.

19.4. Dodavatel prohlašuje, že jím poskytované plnění bude odpovídat všem požadavkům vyplývajícím z platných právních předpisů, které se na plnění této Smlouvy vztahují. V případě, že se toto prohlášení ukáže jako nepravdivé, má Zadavatel vedle práva odstoupit od Smlouvy právo na smluvní pokutu ve výši 500.000,- Kč za každý jednotlivý případ, čímž není nijak dotčen nárok na náhradu škody. Dodavatel není v prodlení, pokud je prodlení způsobeno neposkytnutím dohodnuté součinnosti Zadavatelem.

19.5. V případě porušení závazku mlčenlivosti či ochrany důvěrných informací je Zadavatel oprávněn požadovat kromě náhrady škody zaplacení smluvní pokuty ve výši 500.000,- Kč za každý jednotlivý případ porušení závazku.

19.6. Dodavatel se zavazuje v případě prodlení s plněním poskytnout Zadavateli slevu z ceny plnění ve výši 0,5 % z celkové ceny příslušného plnění (např. objednávky; v případě, že se bude jednat o nesplnění povinnosti, která se vztahuje k plnění, které není samostatně naceněno a tedy spadá do průběžného rozvoje, bezpečnosti a údržby DMS, pak z ceny paušálu atd.) za každý započatý den prodlení.

19.7. Dodavatel se zavazuje v případě využití referenčního prostředí Zadavatele poskytnout Dodavateli slevu ve výši 20.000,- Kč z ceny plnění za každý započatý den využití referenčního prostředí Dodavatele, a to z dodávky DMS, se kterou poskytnutí referenčního prostředí souviselo.

19.8. Dodavatel se zavazuje pro případ nesplnění garantované úrovně záručního servisu poskytnout Zadavateli slevu z ceny resp. smluvní pokuty v případě, že již nebude následovat další fakturace, ve výši 5.000,- Kč za každou započatou hodinu resp. den nedodržení SLA, a to z ceny průběžného rozvoje, bezpečnosti a údržby DMS.

19.9. Dodavatel se zavazuje pro případ neodstranění všech záručních vad spadajících do záručního servisu, které byly Dodavateli nahlášeny včas před ukončením Smlouvy, poskytnout Zadavateli slevu z ceny průběžného rozvoje, bezpečnosti a údržby DMS ve výši 2.000,- Kč za každou jednotlivou neopravenou záruční vadu.

19.10. Dodavatel se zavazuje pro případ prodlení se zajištěním Projektové kanceláře odpovídající požadavkům této Smlouvy poskytnout Zadavateli slevu ve výši 5.000,- Kč za každý započatý pracovní den nesplnění této povinnosti. Sleva bude poskytnuta v rámci fakturace ceny průběžného rozvoje, bezpečnosti a údržby DMS.

19.11. Dodavatel se zavazuje pro případ prodlení se zajištěním funkčního automatického propojení SDM Zadavatele a HelpDesku Dodavatele poskytnout Zadavateli slevu ve výši 5.000,- Kč za každý započatý pracovní den nesplnění této povinnosti. Sleva bude poskytnuta v rámci fakturace ceny průběžného rozvoje, bezpečnosti a údržby DMS.

19.12. Dodavatel se zavazuje pro případ prodlení s pořízením TI potřebné pro realizaci předmětu plnění této Smlouvy poskytnout Zadavateli slevu ve výši 5.000,- Kč za každý započatý pracovní den nesplnění této povinnosti. Sleva bude poskytnuta v rámci fakturace ceny průběžného rozvoje, bezpečnosti a údržby DMS.

19.13. Dodavatel se zavazuje pro případ prodlení s předáním bezpečnostní dokumentace, která je součástí předmětu plnění této Smlouvy dle čl. 2.5.3, poskytnout Zadavateli slevu ve výši 2.500,- Kč za každý započatý pracovní den nesplnění této povinnosti. Sleva bude poskytnuta v rámci fakturace ceny průběžného rozvoje, bezpečnosti a údržby DMS.

19.14. Dodavatel se zavazuje pro případ prodlení s integrací/propojením SW nástroje SpiraTest, s vlastní nástrojem pro podporu / řízení testů poskytnout Zadavateli slevu ve výši 5.000,- Kč za každý započatý pracovní den nesplnění této povinnosti. Sleva bude poskytnuta v rámci fakturace ceny průběžného rozvoje, bezpečnosti a údržby DMS.

19.15. V případě prodlení Zadavatele s placením faktur bude úrok z prodlení stanoven dle příslušného nařízení vlády.

19.16. Sleva z ceny plnění bude zahrnuta do fakturace příslušného plnění, s tím, že maximální výše celkové slevy (resp. součet uplatněných slev daného plnění) může dosáhnout nejvýše 50% z ceny daného plnění. V případě, že již nebude následovat fakturace například z důvodu skončení Smlouvy a poskytnutí slevy tak nebude objektivně možné, má Zadavatel právo požadovat ve stejné výši smluvní pokutu.

19.17. Smluvní pokuta je splatná do patnácti (15) kalendářních dnů ode dne doručení písemné výzvy k jejímu zaplacení.

19.18. Smluvní strany se zavazují vyvinout maximální úsilí k smírnému odstranění a vyřešení sporů, a to zejména prostřednictvím oprávněných osob nebo statutárních orgánů.

19.19. Vznikem nároku na zaplacení smluvní pokuty, poskytnutí slevy z ceny nebo úroků z prodlení, jejich vyúčtováním nebo zaplacením není dotčen nárok smluvní strany na náhradu vzniklé škody.

19.20. Pokud není uvedeno jinak, jsou částky v Kč v tomto článku uvedeny vždy bez DPH.

20. PRAVIDLA PRO UPŘESŇOVÁNÍ ROZSAHU PLNĚNÍ DÍLČÍMI OBJEDNÁVKAMI

20.1. Smluvní strany mohou uzavírat objednávky, na základě kterých bude upřesňován předmět plnění podle čl. 2.5.2.

20.2. Objednávky budou uzavírány jako smlouvy o dílo v souladu ustanoveními § 2586 a násl. občanského zákoníku. Bude-li součástí objednávky i poskytnutí licencí standardního software třetích stran, bude se při jejich poskytnutí smluvní vztah řídit ustanoveními § 2358 a násl. občanského zákoníku jako licenční smlouva. Bude-li součástí objednávky i dodávka hardware, bude se při dodávce hardware smluvní vztah řídit ustanoveními § 2079 a násl. občanského zákoníku jako kupní smlouva. Uvedená ustanovení o licenční a kupní smlouvě nemění nic na zodpovědnosti Dodavatele předat plnění podle příslušné objednávky jako funkční dílo.

20.3. Nestanoví-li objednávka výslovně jinak, řídí se práva a povinnosti smluvních stran touto Smlouvou. V případě rozporu mezi zněním této Smlouvy a zněním objednávky platí ustanovení objednávky. Změny provedené objednávkou oproti ustanovením této Smlouvy nebo její doplnění se mohou týkat pouze plnění poskytovaného na základě takové objednávky a tyto změny či doplnění musí být v souladu s právními předpisy upravujícími zadávání veřejných zakázek. Smluvní strany nejsou oprávněny uzavřít objednávky způsobem či za podmínek, které jsou v rozporu s příslušnými právními předpisy.

20.4. Ukončení účinnosti kterékoliv objednávky nemá vliv na platnost ani účinnost této Smlouvy.

21. MOŽNOSTI ODSTOUPENÍ OD SMLOUVY A VÝPOVĚDI SMLOUVY

21.1. Účinnost této Smlouvy lze předčasně ukončit:

21.1.1. písemnou dohodou smluvních stran, jejíž součástí je i vypořádání vzájemných závazků a pohledávek; rozpracované objednávky budou dokončeny, nedohodnou-li se smluvní strany jinak;

21.1.2. ze strany Zadavatele písemným odstoupením od Smlouvy či objednávky z důvodu jejího podstatného porušení Dodavatelem (odstoupení od Smlouvy ze strany Zadavatele nesmí být spojeno s uložením jakékoliv sankce k tíži Zadavatele), přičemž za podstatné porušení Smlouvy či objednávky se bude považovat zejména, nikoliv však výlučně, prodlení Dodavatele s předáním předmětu plnění (či jeho dílčí části) delší než 30 dnů, a dále porušení jakékoliv podstatné povinnosti Dodavatele vyplývající z této Smlouvy či objednávky a její nesplnění ani v dodatečné přiměřené lhůtě, kterou Zadavatel Dodavateli k tomu poskytne (nevylučuje-li to charakter porušené povinnosti); v pochybnostech se má za to, že dodatečná lhůta je přiměřená, pokud činila alespoň 5 dnů.

21.1.3. ze strany Dodavatele písemným odstoupením od Smlouvy dle příslušných ustanovení občanského zákoníku.

21.1.4. vypovědí kterékoliv ze stran bez udání důvodu s výpovědní lhůtou 6 měsíců, která běží počínaje následujícím měsícem od měsíce, v němž byla výpověď druhé straně doručena.

21.2. Odstoupením od této Smlouvy nebo výpovědí Smlouvy nejsou dotčena ustanovení týkající se náhrady škody, smluvních pokut, slev z ceny, ochrany informací, zajištění pohledávky kterékoliv ze stran, řešení sporů a ustanovení týkající se těch práv a povinností, z jejichž povahy vyplývá, že mají trvat i po odstoupení nebo výpovědi Smlouvy (zejména jde o povinnost poskytnout peněžitá plnění za plnění poskytnutá před účinností odstoupení).

22. PŘECHOD VLASTNICKÝCH PRÁV A PŘEVOD PRÁV K UŽITÍ A ŠÍŘENÍ AUTORSKÉHO DÍLA

22.1. Dodavatel bude mít po podpisu této Smlouvy ve svém držení výstupy potřebné k zajištění rozvoje a údržby DMS, a to zejména v tomto rozsahu:

22.1.1. kompletní zdrojové kódy;

22.1.2. skripty pro generování databázových schémat;

22.1.3. další pomocné soubory (instalační skripty apod.);

22.1.4. export repository pro Enterprise Architect;

22.1.5. existující dokumentace, popis verzí a nastavení nástrojů používaných pro vývoj, údržbu a provoz systému;

22.1.6. principy monitorování a aktualizace požadavků;

22.1.7. stávající bezpečnostní dokumentace;

22.1.8. systémová příručka IS.

22.2. Dodavatel se zavazuje, že nepoužije výstupy dle čl. 22.1. nebo jejich části a dále know-how získané z výstupů DMS pro jiné účely, než pro další rozvoj a údržbu DMS v rámci působnosti resortu Zadavatele, v souladu s účelem této Smlouvy.

22.3. Vlastnické právo k hmotným součástem díla (či jeho dílčí části) přechází na Zadavatele uhrazením ceny za takové hmotné součásti díla (či jeho dílčí části). Nebezpečí škody na hmotných součástech díla (či jeho dílčí části) přejde z Dodavatele na Zadavatele dnem protokolárního převzetí hmotných součástí díla (či jeho dílčí části) a Zadavateli zároveň vznikne právo hmotné součásti díla (či jeho dílčí části) užívat v souladu s účelem této Smlouvy.

22.4. Dodavatel se zavazuje, že pokud součástí díla bude i plnění, které naplňuje znaky díla ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, získává Zadavatel oprávnění k výkonu majetkových práv k takovému dílu, a to podle ustanovení § 12 a násl. autorského zákona, tedy právo k užití díla (dále jen „licenci“) specifikované níže:

22.4.1. výhradní licence k veškerým známým způsobům užití takového díla, zejména, nikoliv však výlučně k účelu, ke kterému bylo takové dílo Dodavatelem vytvořeno v souladu se Smlouvou;

22.4.2. neomezený územní či množstevní rozsah licence;

22.4.3. licence udělená po celou dobu trvání majetkových práv k dílu;

22.4.4. licence je udělena s právem udělení podlicence jakékoliv třetí osobě;

22.4.5. licenci není Zadavatel povinen využít.

22.5. Dodavatel prohlašuje, že vlastní veškerá oprávnění k dílu dle čl. 22.4., zejména, nikoliv však výlučně, že disponuje majetkovými právy k dílu, resp. oprávněním k jejich výkonu a je oprávněn je poskytnout Zadavateli (zejména tedy uzavřel či uzavře pracovní či jiné smlouvy, na základě kterých se stane vykonavatelem majetkových práv autorských k dílu s právem postoupeni práva výkonu majetkových práv autorských).

22.6. Dodavatel prohlašuje, že užitím díla dle čl. 22.4. Zadavatelem nebudou neoprávněně porušena ani jiná práva a oprávněné zájmy třetích osob, zejména právo na ochranu osobnosti fyzických osob a právo na ochranu dobré pověsti právnických osob.

22.7. Dodavatel prohlašuje, že dle ustanovení § 12 odst. 4 autorského zákona je Zadavatel oprávněn ke všem způsobům užití díla dle čl. 22.4., tj. zejména dílo užít jeho zpřístupněním veřejnosti, vystavením, zveřejněním v síti internet. Zadavatel je oprávněn šířit dílo v elektronické, tištěné i jiné podobě. Zadavatel může dílo využít ke komerčním i nekomerčním účelům, dále upravovat, zpracovávat, překládat, či měnit jeho název, spojit s jiným dílem a zařadit jej do díla souborného bez předchozího souhlasu autora, včetně poskytnutí tohoto díla k úpravám smluvním partnerům Zadavatele. Za tímto účelem se Dodavatel zavazuje předat Zadavateli veškeré zdrojové kódy k takovému dílu, včetně související dokumentace a to tak, že budou uloženy na k tomu vyhrazených datových prostředcích Zadavatele nebo mu budou nejpozději k datu předání díla nebo jeho části předány na datovém nosiči (CD/DVD).

22.8. Veškerá oprávnění poskytnutá Zadavateli dle čl. 22. jsou již zahrnuta v ceně za poskytnuté plnění dle této Smlouvy.

22.9. Udělení veškerých práv uvedených v čl. 22. nelze ze strany Dodavatele vypovědět a rovněž tak na udělení takových práv nemá vliv ukončení platnosti této Smlouvy.

22.10. Ustanovení čl. 22. se nevztahují na poskytnutí licencí počítačových programů – standardního licencovaného software, které existovaly již před podáním nabídky Dodavatele na Veřejnou zakázku a byly již vícenásobně poskytnuty jiným zákazníkům jako nevýhradní licence. Licenční podmínky takového software budou součástí příslušné dílčí objednávky, v rámci jejíž plnění budou licence poskytnuty.

22.11. Dodavatel není oprávněn použít takový nekomerční/Open Source SW, jehož začleněním do IS DMVS resp. díla by tento ztratil svůj proprietární charakter (tj. jestliže by podle licenčních podmínek takového nekomerčního/Open Source SW jeho začleněním do IS DMVS došlo k povinnosti zpřístupnit IS DMVS pod tzv. svobodnou licenci/licencí copyleft).

23. KOORDINACE S DALŠÍMI PROJEKTY ZADAVATELE

23.1. Dodavatel plně garantuje, že bude aktivně spolupracovat či poskytne součinnost dodavatelům a výrobcům stávající technologické infrastruktury, programového vybavení a souvisejících či spolupracujících interních či externích aplikací či informačních systémů.

23.2. Dodavatel se dále zavazuje, že bude spolupracovat či poskytne součinnost případným dodavatelům Zadavatele, jejichž plnění bude souviset s plněním podle této Smlouvy, zejména GC System s.r.o., Oracle Czech, s.r.o, NESS Czech s.r.o., aplis.cz, a.s., Kentico Software s.r.o., Sefira spol. s.r.o.,awin IT, s. r. o., Microsoft s.r.o., CCA Group a.s, a to za podmínky, že Zadavatel zajistí požadovanou spolupráci těchto dodavatelů s Dodavatelem.

23.3. Dodavatel se zavazuje, že v případě potřeby uzavře, za účelem předání relevantních informací pro porozumění programátorské dokumentaci na úrovni modulů i celých aplikací, případně konzultací k datovému modelu, smlouvu s dodavatelem, který bude vybrán Zadavatelem pro rozvoj a údržbu DMS pro další období po skončení této Smlouvy. Pro takovou smlouvu bude maximální možná jednotková cena odpovídat ceně uvedené v čl. 15.2., položce 1.

24. JINÁ USTANOVENÍ

24.1. Smluvní vztah mezi smluvními stranami se řídí českým právním řádem. Právní vztahy mezi smluvními stranami založené touto Smlouvou a zvlášť v ní neupravené se řídí občanským zákoníkem, autorským zákonem a zákonem o zadávání veřejných zakázek.

24.2. Jakékoliv změny či doplnění Smlouvy je možné činit výhradně formou písemných, datovaných a číselně označených dodatků ke Smlouvě podepsaných oběma smluvními stranami.

24.3. Smluvní strany se dohodly, že bez předchozího výslovného písemného souhlasu druhé strany nepostoupí ani nepřevedou jakákoliv práva či povinnosti vyplývající z této Smlouvy na třetí osobu či osoby.

24.4. Vztahuje-li se důvod neplatnosti jen na některé ustanovení Smlouvy, je neplatným pouze toto ustanovení, pokud z jeho povahy nebo obsahu anebo z okolností, za nichž bylo sjednáno, nevyplývá, že jej nelze oddělit od ostatního obsahu této Smlouvy.

24.5. Veškeré případné spory z této Smlouvy budou řešeny věcně a místně příslušným soudem v České republice.

24.6. Jednacím jazykem mezi Zadavatelem a Dodavatelem bude pro veškerá plnění vyplývající ze Smlouvy výhradně jazyk český, a to včetně veškeré dokumentace vztahující se k předmětu této Smlouvy.

24.7. Smluvní strany berou na vědomí, že tato Smlouva podléhá zveřejnění dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).

25. ZÁVĚREČNÉ USTANOVENÍ

25.1. Tato Smlouva je vyhotovena v jednom vyhotovení v elektronické podobě.

25.2. Nedílnou součástí této Smlouvy jsou přílohy:

Číslo Přílohy Smlouvy	Obsah přílohy Smlouvy	Přílohu vyhotovil
1	Seznam použitých pojmů a zkratek	Zadavatel
2	Personální zajištění Smlouvy	Zadavatel a Dodavatel
3	Průběžný rozvoj a údržba DMS	Zadavatel
4	Systém pro evidenci požadavků	Dodavatel
5	Metodika interního testování dodávek DMS	Dodavatel
6	Způsob a metodika vývoje	Dodavatel
7	Vedení dokumentace – projektová kancelář	Dodavatel
8	Práva a povinnosti manažera a architekta kybernetické bezpečnosti VIS	Zadavatel
9	Seznam bezpečnostní dokumentace pro DMS	Zadavatel
10	Zajištění bezpečnostních testů	Zadavatel

Datum: dle elektronického podpisu
Za Zadavatele:

[redacted]

Podpis: Viditelný elektronický podpis
Jméno: [redacted]
Funkce: místopředseda ČÚZK

Datum: dle elektronického podpisu
Za Dodavatele:

[redacted]

Podpis: Viditelný elektronický podpis
Jméno: [redacted]
Funkce: Místopředsedkyně představenstva

Seznam použitých pojmů a zkratek

Zkratka, pojem	Vysvětlení
CR	1. Change request, požadavek na změnu/dokument popisující způsob řešení změnového požadavku; 2. v kontextu RPP je zkratka používána pro činnostní roli
ČR	Česká republika
ČLD	Člověkoden, tj. 8 hodin práce jedné osoby
ČSN	Chráněné označení českých technických norem
ČÚZK	Český úřad zeměměřický a katastrální
DB	Databáze
DMS	Document Management systém
DP	Dálkový přístup, www rozhraní ISKN pro externí uživatele
DPH	Daň z přidané hodnoty
DS	Datová schránka
eIDAS	Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, které bylo publikováno v Úředním věstníku Evropské unie dne 23. července 2014.
EPVDS	Elektronická podatelna a výpravna datových schránek
EU	Evropská unie
FAKE komponenta	Zastupující komponenta určena převážně pro účely testování, simuluje činnost pravé komponenty. Má stejné rozhraní, ale jinou vnitřní funkčnost. Například simulované zasílání SMS zpráv namísto skutečného zasílání přes SMS bránu.
GUI DMS	Webové rozhraní DMS
HD	HelpDesk
IČO	Identifikační číslo osoby
ID DS	Identifikátor datové schránky
IEEE	Institute of Electrical and Electronics Engineers (Institut pro elektrotechnické a elektronické inženýrství)
IETF	Internet Engineering Task Force (Komise techniky Internetu)
IS	Informační systém
ISKN	Informační systém katastru nemovitostí
ISO	International Organization for Standardization
ISP	Identifikace a specifikace požadavků
ISVS	Informační systémy veřejné správy
ISZR	Informační systém základních registrů
KESSL	Komplexní elektronická spisová služba
KN	Katastr nemovitostí
MTOM	Message Transmission Optimization Mechanism
NBD	Next business day (Další pracovní den)
.NET	Microsoft Net Framework
OB-TA	Obelisk trusted archive
PDF	Portable Document Format (Přenosný formát dokumentů)
PK	Projektová kancelář
PROD	Produkční prostředí
ŘV	Řídící výbor, nejvyšší orgán řízení projektu
SDM	Service Desk Manager, systém evidence problémů / požadavků

SK	Školení
SLA	Service Level Agreement, definice rozsahu dostupnosti služeb
SP	Servisní požadavek
SpiraTest	SW nástroj pro řízení testů na straně Zadavatele, verze 5.4.0.4
SW	Software
tel.	Telefon
TI	Technologická infrastruktura
TP	Technická podpora
VV	Výkonný výbor, orgán řízení projektu
VZ	Veřejná zakázka
WS	Web Services, webové služby
WSDL	Web Services Description Language, XML popis WS
WWW	Word Wide Web
XML	eXtensible Markup Language, rozšiřitelný značkovací jazyk pro tvorbu strukturovaných dat
ZD	Zadávací dokumentace Veřejné zakázky „Rozvoj a údržba DMS v letech 2021 – 2025“
ZoISVS (Standard ISVS)	Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů a prováděcí předpisy vydané na jeho základě
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů

Příloha č. 2 Smlouvy

Personální zajištění Smlouvy

Role	Zadavatel	Dodavatel
Oprávněné osoby	[redacted]	[redacted]
Zástupci oprávněných osob	[redacted]	[redacted]
Členové Řídícího výboru	[redacted]	[redacted]
Ředitel Projektu	[redacted]	[redacted]
Vedoucí Projektu	[redacted]	[redacted]
Vedoucí týmu bezpečnosti	[redacted]	[redacted]

Projektový manažer Dodavatele	[redacted]
Hlavní/systémový architekt Dodavatele	[redacted]
Vývojář informačních systémů Dodavatele	[redacted]
Databázový administrátor	[redacted]
Specialisté na bezpečnost (manažer a architekt kybernetické bezpečnosti)	[redacted]
Specialista pro řízení servisních služeb podpory	[redacted]

Příloha č. 3 Smlouvy

Průběžný rozvoj, bezpečnost a údržba DMS

Rozvojem DMS se rozumí modifikace částí existujícího systému nebo vytvoření nové části systému, spočívající zejména v zapracování potřebných změn, vyplývajících ze změny právních předpisů (zejména změn týkajících se eIDAS a zákonů č. 499/2004 Sb., zákon o archivnictví a spisové službě a č. 365/2000 Sb., zákon o informačních systémech veřejné správy a o změně některých dalších zákonů), požadavkům z oblasti kybernetické bezpečnosti v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, a přizpůsobení DMS požadavkům vzniklým z funkčnosti ostatních informačních systémů napojených na DMS. Mezi další rozvojové požadavky patří optimalizace uložení a načítání dat. Dále se jedná o udržování aktuálních verzí použitých technologií, zejména přechodem na nejnovější aktuální a stabilní verze databázové a aplikační části informačního systému před ukončením Smlouvy, provedení DR testu, zajištění převodu obsahů dokumentů do výstupní datového formátu dokumentů v digitální podobě, pokud dokument na vstupu v tomto formátu nebude a zajištění validního skartačního procesu pro spisovou službu katastrálních pracovišť.

Rozvojem se rozumí i taková úprava DMS, ve které se do systému nezavádí zcela nová funkčnost, ale požadují se takové úpravy, které povedou ke stabilizaci, případně optimalizaci stávajícího řešení.

Požadavky na průběžný rozvoj, bezpečnost a údržbu DMS

Průběžná údržba znamená řešení a odstraňování provozních problémů a havárií tak, aby z důvodu omezené funkčnosti nebo nedostupnosti DMS nebyl v žádném okamžiku ohrožen řádný výkon státní správy v zeměměřictví a katastru nemovitostí zajišťovaný Zadavatelem. Průběžná údržba zahrnuje identifikaci a kategorizaci požadavků a následné opravy DMS zařazené do příslušné verze DMS. Identifikací požadavku se rozumí analýza příčin problému nahlášeného Zadavatelem, včetně návrhu základního způsobu řešení bez ohledu na to, zda se jedná o závadu systému DMS, HW, souvisejícího SW nebo jinou závadu. Kategorizací se rozumí stanovení, zda jde o závadu DMS, a to buď v části, která nebyla modifikována v rámci plnění dle této Smlouvy, nebo v části již modifikované v rámci plnění dle této Smlouvy.

V rámci průběžné údržby budou vyřešeny opravy nesprávné funkčnosti DMS (např. rozdílné chování proti uživatelské příručce) v částech nemodifikovaných v rámci plnění dle této Smlouvy (mimozáruční závady). Vyřešením se, s výjimkou kritických závad, pro tyto účely rozumí zařazení dané opravy/oprav do nejbližší následující verze DMS, nebude-li v rámci vedení projektu dohodnuto jinak.

Dodavatel bude poskytovat paušální služby průběžného rozvoje DMS do celkového rozsahu 10 člověkodní (dále také „ČLD“) měsíčně, služby průběžné údržby do celkového rozsahu 10 ČLD měsíčně a služby zajišťující bezpečnost informačního systému do celkového rozsahu 2 ČLD měsíčně.

Zadavatel v této souvislosti požaduje, aby Dodavatel v předstihu před fakturací za průběžný rozvoj, bezpečnost a údržbu předkládal Zadavateli k odsouhlasení měsíční výkazy a přehledy s výsledky průběžného rozvoje, údržby a bezpečnosti. Kumulované nevyčerpané ČLD z předchozích měsíců, maximálně však celkem 10 ČLD za služby průběžného rozvoje, 10 ČLD za služby průběžné údržby a 2 ČLD za služby zajišťující bezpečnosti informačního systému, bude možné převádět do následujícího měsíce. Kumulaci nevyčerpaných ČLD je možné realizovat nejvýše v rámci jednoho fakturačního čtvrtletí poskytování služby. Průběžný rozvoj, údržba a bezpečnost DMS budou Dodavatelem vykazovány Zadavateli 1 x měsíčně ve výkazu.

V případě, že měsíční čerpání ČLD v jedné z oblastí rozvoje, údržby, či bezpečnosti dosáhne 90% měsíčního paušálu, Dodavatel kontaktuje Zadavatele, který rozhodne, zda je možné daný měsíc přečerpat měsíční paušál v dané oblasti, či se realizace z dané oblasti odloží do následujícího měsíce.

Mimozáruční kritické závady budou řešeny se stejným SLA jako kritické závady spadající do záručního servisu.

Opravy nesprávné funkčnosti DMS v částech modifikovaných v rámci plnění dle této Smlouvy (dále jen „záruční závada“) budou provedeny zdarma v rámci záručního servisu, a to za podmínek uvedených v této Smlouvě.

Instalace opravných skriptů či oprav kritických, závažných nebo bezpečnostních chyb/zranitelností budou probíhat urychleně bez vazby na dodávku.

Záruční závady, které budou Zadavatelem nahlášeny před ukončením doby plnění dle Smlouvy v termínu delším než je jejich doba vyřešení, viz tabulka níže, je Dodavatel povinen odstranit v těchto požadovaných dobách. Záruční vady, u nichž požadovaná doba vyřešení uplyne s ohledem na okamžik jejich nahlášení až po skončení Smlouvy, není Dodavatel povinen odstranit.

Požadavky na záruční servis

Základní parametry záručního servisu

Zadavatel požaduje, aby Dodavatel zajištěný záruční servis splňoval minimálně tyto uvedené parametry:

a) záruční doba činí 2 roky od akceptace daného plnění, zároveň však nejdéle do konce uzavřené Smlouvy;

b) záruční servis bude poskytován od pondělí do pátku v době od 6:00 do 18:00. Je-li požadováno odstranění závady NBD, považuje se závada za včas odstraněnou za předpokladu, že bude odstraněna do následujícího pracovního dne do 16:00. Doba reakce a vyřešení běží pouze pokud byla nahlášena v době pokrytí – v hodinách poskytování záručního servisu;

c) poskytnutá záruka se vztahuje na všechny části díla, včetně příslušenství;

d) záruka se vztahuje na funkčnost díla, jakož i na vlastnosti, požadované Zadavatelem;

e) záruka se prodlužuje o dobu, po kterou mělo dílo závadu bránící jeho řádnému užívání Zadavatelem;

f) veškeré zjištěné nedostatky, nedodělky a závady díla, které se vyskytnou v záruční době, je Dodavatel povinen odstranit na své náklady v termínech uvedených níže po jejich oznámení Zadavatelem. Pokud se bude jednat o požadavek spadající do průběžné provozní údržby se stupněm závažnosti 1 (kritická závada), bude řešen dle příslušné SLA také na náklady Dodavatele;

g) Dodavatel musí vždy provést řádnou identifikaci požadavku, včetně návrhu základního způsobu řešení bez ohledu na to, zda se jedná o závadu systému DMS, HW, souvisejícího SW nebo jinou závadu. Ukáže-li se však později, že provedená identifikace a kategorizace závady byla ze strany Dodavatele chybná a o závadu DMS se jednalo, počítá se SLA a případné sankce za její nedodržení od původního okamžiku nahlášení;

h) pokud se nebude jednat o chybu DMS spadající do záručního servisu, ale bude se jednat o chybu DMS a toto zjištění bude oboustranně odsouhlaseno, bude požadavek dále řešen buď v rámci průběžné provozní údržby, případně v rámci provozní údržby na objednávku;

i) Dodavatel odpovídá Zadavateli za případnou škodu, která mu vznikne z titulu neodstranění závady díla ve sjednaném termínu;

j) pro případy, kdy odstranění závady není ve sjednané lhůtě objektivně možné, navrhne Dodavatel Zadavateli náhradní řešení, které bude co nejvíce eliminovat případnou škodu Zadavatele;

k) pokud se Dodavatel rozhodne v DMS využít nekomerční (Open Source) SW, vztahuje se záruka i na něj,

Rozsah záručního servisu
Zadavatel požaduje, aby v rámci záručního servisu Dodavatel prováděl:

1. identifikaci a kategorizaci nahlášených závad,
2. odstraňování závad DMS modifikovaného v rámci plnění dle této VZ a kritických závad bez omezení,
3. konfigurační řízení pro odstraňování identifikovaných závad, zejména verzování, příprava instalačních zdrojů, ….

Klasifikace chyb / stupeň závažnosti
Každý Zadavatelem ohlášený požadavek kategorie „CCA závada“ na odstranění závad DMS bude ohodnocen stupněm závažnosti ze strany Zadavatele.

Pro stanovení závažnosti závady bude používána klasifikace dle níže uvedených stupňů závažnosti závad:

Stupeň závažnosti	Klasifikace chyby	Popis závady / dopad závady na činnosti Zadavatele
1	Kritická závada	DMS není použitelný ve svých základních funkcích nebo se vyskytuje funkční závada znemožňující práci s DMS z důvodu, že některá aplikace nebo její část je zcela nefunkční a požadovanou činnost nelze realizovat jinak, nebo stav DMS umožňuje porušení konzistenci dat, nebo systém DMS vykazuje sníženou výkonnost, tj. průměrná doba vybavení metadat/dokumentu v rámci jedné hodiny přesahuje 3 sekundy, platí pro dokumenty vybavované z diskového úložiště. Za kritickou chybu se považují také případy, kdy závažná chyba spočívající ve snížené výkonnosti DMS přetrvává déle než 3 pracovní dny. Kritická závada je také v případě, že se nepodaří otevřít minimálně pět dokumentů z páskového uložiště během jedné hodiny. Time out pro vybavení jednoho dokumentu z páskového uložiště je nastaven na pět minut. Dopad: Bezprostředně ohrožuje činnost Zadavatele jako orgánu státní správy nebo jeho povinnosti vyplývající ze zákona.
2	Závažná závada	Modul nebo jeho část je nefunkční, požadovanou činnost lze realizovat náhradním způsobem nebo modul povoluje vykonat nepovolenou činnost nebo některé funkce modulu nefungují korektně, ale základní funkčnost je zajištěna, nebo systém DMS vykazuje sníženou výkonnost, tj. průměrná doba vybavení metadat/dokumentu v rámci jedné hodiny přesahuje 1,5 sekundy, platí pro dokumenty vybavované z diskového úložiště. Závažná závada je také v případě, že se nepodaří otevřít minimálně tři dokumenty z páskového uložiště během jedné hodiny. Time out pro vybavení jednoho dokumentu z páskového uložiště je nastaven na pět minut. Nemůže dojít k nekonzistencím v datech. Dopad: V časovém horizontu do 1 týdne může ohrozit činnost Zadavatele jako orgánu státní správy nebo jeho povinnosti vyplývající ze zákona.
3	Závada	Některé funkce DMS pracují omezeně, případně modul nereaguje správně na chybné akce uživatele, poskytuje nesrozumitelná chybová hlášení, chyby uživatele nejsou indikovány okamžitě. Nemůže dojít k nekonzistencím v datech. Dopad: Bezprostředně neohrožuje činnost Zadavatele jako orgánu státní správy nebo jeho povinnosti vyplývající ze zákona.
4	Drobná závada	Nedostatky DMS do určité míry komplikující nebo neumožňující jeho plnohodnotné využití. DMS neposkytuje jasná chybová či informativní hlášení nebo je naopak vypisuje na místě, kde by se vyskytnout neměla. V popisném textu položky (prompt), řádkové nápovědě (hint), místní nápovědě (tooltip), v názvu položky menu nebo v textu nápovědy se vyskytuje překlep, pravopisná chyba apod. Správná funkčnost a konzistence dat je zajištěna.

		Dopad: Neohrožuje činnost Zadavatele jako orgánu státní správy nebo jeho povinnosti vyplývající ze zákona.

Doby vyřešení (SLA)

V závislosti na stupni závažnosti závady požaduje Zadavatel níže uvedené reakční doby a dodání řešení.

Stupeň závažnosti	Klasifikace závady	Reakční doba	Doba vyřešení
1	Kritická závada	1 hodina	4 hodiny
2	Závažná závada	2 hodiny	NBD
3	Závada	3 pracovní dny	10 pracovních dnů
4	Drobná závada	5 pracovních dnů	30 pracovních dnů

Požadavky na zajištění průběžné bezpečnosti DMS

Při realizaci předmětu plnění musí Dodavatel garantovat zachování bezpečnosti DMS, pokud nějaký právní předpis nepožaduje vyšší bezpečnost, tak alespoň na stávající úrovni.

DMS je informačním systém veřejné správy dle zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů (dále jen „ZoISVS“).

DMS se stane od 1.1.2022 Významným informačním systémem v souladu s novelizovanou vyhláškou 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích. Zadavatel předpokládá, že Dodavatel se stane významným dodavatelem dle zákona 181/2014 Sb. (ZoKB) a vyhlášky o kybernetické bezpečnosti 82/2018 Sb. (VoKB).

Požadované průběžné činnosti Dodavatele v oblasti bezpečnosti:

a) řízení bezpečnosti DMS a odpovědnosti za splnění zákonných požadavků a povinností, týkajících se DMS v této oblasti, kladených na orgán veřejné správy, po celou dobu plnění.

b) navrhování doplnění a změn platných vnitřních předpisů včetně organizačních opatření,

c) aktualizace havarijního plánu (tj. plánu obnovy) DMS včetně postupů při obnově provozu DMS. Průběžné zapracovávání změn a řešení nedostatků zjištěných při ověření havarijního plánu Zadavetelem. Před schválením aktualizace havarijního plánu je, při rozhodnutí o ověření (testování) jejich funkčnosti, Dodavatel povinen poskytnout Zadavateli součinnost.

d) vytváření dokumentu popisujícího životní cyklus řízení přístupu k logům DMS a způsob zacházení s nimi, tj. popisující jaké logy jsou v rámci DMS a v souvislosti s ním DMS vytvářeny, o jaký typ logů se jedná, nastavení logování, jak dlouho se mají logy ukládat, jejich odmazávání, provádění záloh, jak dlouho mají být archivovány, kde a zda a jaké činnosti jsou prováděny automaticky či je nutný zásah bezpečnostního správce.

e) zajišťování toho, aby před nasazením nové verze DMS do provozního prostředí byly provedeny bezpečnostní testy DMS, s tím, že nalezené kritické zranitelnosti v oblasti bezpečnosti musí být napraveny a opakovaně ověřeny před nasazením dané úpravy/dodávky do provozního prostředí Zadavatele. Dokument Metodika provádění bezpečnostních testů předloží Dodavatel před první změnou DMS. Dodavatel požaduje, aby testy prováděl Dodavatel. Výsledky bezpečnostních testů Dodavatel zpracuje do dokumentu Zpráva o výsledcích bezpečnostních testů DMS a předloží je

s návrhy opatření a uvedením způsobu, jakým byly zjištěné kritické zranitelnosti vyřešeny Zadavateli.

f) na základě zranitelností zjištěných při dalších bezpečnostních testech, auditech, externích penetračních testech a na základě kritických událostí vedoucích k výpadkům DMS musí Dodavatel zajistit realizaci opatření, schválených Zadavatelem na odstranění těchto zranitelností, pokud jsou tyto zranitelnosti zapříčiněny jeho plněním. Dodavatel musí dále navrhnout opatření v oblasti bezpečnosti, k odstranění zranitelností, plněním Dodavatelem přímo nezpůsobeným.

g) účast na schůzce minimálně 1x za 6 týdnů v sídle Zadavatele k zajištění bezpečnosti DMS, které svolá Dodavatel. Na schůzkách bude Dodavatel informovat o aktuálním stavu plnění činností, předkládat k připomínkám návrhy dokumentů a jejich změn, případně konzultovat návrhy opatření, tak aby jeho činnost směrovala k akceptaci předkládaných dokumentů Zadavatelem. Ze schůzek pořizuje Dodavatel zápisy, které zasílá k připomínkám styčnému zaměstnanci pro oblast bezpečnosti za Zadavatele.

h) navrhnutí, zajištění a vyžadování bezpečné elektronické komunikace mezi jím a Zadavatelem při předávání informací, dokumentů, řešení bezpečnosti a dalších činností v oblasti bezpečnosti prostřednictvím veřejné datové sítě.

i) vytvoření a aktualizování dokumentu Bezpečnost a řízení přístupu do PK. Dokument musí popisovat minimálně řízení přístupu do PK, řízení přístupu k různým kategoriím dokumentů z hlediska bezpečnosti (standardní, důvěrné, …), popis zajištění logování a auditu přístupů do PK k jednotlivým dokumentům.

Požadavky na monitorování provozu

Zadavatel požaduje, aby součástí plnění Dodavatele (při dodávkách nových verzí DMS, případně i při instalacích opravných patchů) bylo i předání monitorovacích nástrojů (skriptů) pro monitorování provozu, a to zejména v období před instalací nové verze DMS do provozního prostředí, s tím, že monitorovány budou zejména oblasti/aplikace DMS, které jsou v rámci dané verze podstatnějším způsobem modifikovány, či v období po zavádění zcela nové funkčnosti. Dodavateli bude umožněn přístup ke čtení pro DMS PROD, na základě tohoto práva bude možné provádět monitoring i na straně Dodavatele. Ze strany Dodavatele budou Zadavateli v dostatečném časovém předstihu před zahájením monitorování provozu poskytnuty/předány použité monitorovací nástroje (skripty) včetně doprovodné dokumentace tak, aby byl Zadavatel schopen zajistit monitorování provozu i vlastními silami, a to minimálně v rozsahu prováděném Dodavatelem.

Zadavatel požaduje, aby řešení, nabízené Dodavatelem pro monitorování provozu, umožňovalo monitorování minimálně následujících metrik:

Popis
Zatížení CPU v %
Obsazená RAM v %
Zbývající místo na disku v %
Odezva hosta v ms a zároveň výpadky v %
Kontrola textu na stránce a zároveň vrácení stránky v sekundách
Obsazené místo ASM diskgrupa v %
Invalidní objekty v kusech
Obsazené místo DB v %
Využití procesů DB v %

Aplikační test - kontrola procesu importu dokumentů ze Samba serveru
Aplikační test - kontrola logu komunikace DMS s OB-TA
Aplikační test - kontrola počtu zpráv odeslaných do OB-TA, jejichž přijetí v OB-TA není potvrzené
Aplikační test běhu aplikace pro odesílání dokumentů z DMS do OB-TA
Aplikační test běhu aplikace pro import dokumentů přes Sambu
Test, který porovnává synchronizaci gridu, při nesrovnalostech rovnou critical
Volné místo pro DB, kam se ukládají zálohy
Test počtu chyb v posledních několik zálohách

Monitoring komunikace pro funkčnosti s externími IS, kdy tyto IS vyvolávají komunikaci (vytváří požadavek) a DMS jim odpovídá, je na straně těchto IS.

Monitoring komunikace pro funkčnosti s externími IS, kdy komunikaci vyvolává (vytváří požadavek) DMS a IS mu odpovídají, je na straně DMS. V případě zavedení nových napojení, kdy komunikaci vyvolává DMS a IS mu odpovídá, bude požadována realizace monitoringu i této komunikace.

Projektové vedení a eskalační proces

Zadavatel požaduje, aby se po celou dobu plnění scházel minimálně jednou měsíčně Řídící výbor (ŘV), jednou za 14 dní Výkonný výbor (VV) a jednou za šest týdnů Bezpečnostní výbor (BV), a to v budově Zadavatele. Bližší pravidla řízení projektu (jednotlivé řídící struktury včetně obsazení ŘV, VV a BV, odpovědnost, postupy odsouhlasování zápisů atd.) si smluvní strany dohodnou nejpozději do 1 měsíce po podpisu Smlouvy.

Pro řešení případných problémů vzniklých v průběhu plnění bude použit následující eskalační mechanismus:

V případě nedohody na VV a BV je problém či spor eskalován na úroveň ŘV. Pokud nedojde k vyřešení sporu či problému na úrovni ŘV, je dalším eskalačním jednáním jednání oprávněných osob Zadavatele i Dodavatele, které mohou předložit návrh řešení problému či sporu následujícímu ŘV. Pokud ani po takovém procesu nedojde ke shodě a některá ze stran požaduje dořešení problému či sporu, budou tento předložen k řešení místně příslušnému soudu.

Systém evidence požadavků

1 Popis systému, ve kterém budou řešeny vady/požadavky/dotazy na straně Dodavatele

Systémem, ve kterém budou řešeny vady/požadavky/dotazy, rozumíme komplex procesů podpořený informačním systémem HelpDesk dodavatele.

V následujících kapitolách postupně popíšeme základní komponenty tohoto systému:

- Služba Helpdesk (vstupní bod systému)
- Hlášení, proces jeho přijetí a zpracování
- Informační systém HelpDesk

V závěrečné kapitole se potom nachází samostatný popis zajištění automatizovaného propojení s SDM Zadavatele.

1.1 Služba Helpdesk

Dodavatel bude provozovat službu HelpDesk jako primární kontaktní bod mezi Zadavatelem a Dodavatelem.

Tuto službu bude zajišťovat po celou dobu účinnosti Servisní smlouvy. Zadavatel bude moci telefonicky komunikovat za v místě a čase běžné hovorné a zadávat své požadavky e-mailem či po přihlášení na registrovaný účet přes webovou aplikaci HelpDesk. Poskytnutá telefonní linka pro přímou podporu Zadavatele bude dostupná v českém jazyce v každý pracovní den od 06:00 do 18:00 hodin.

Helpdesk	
Provozní doba	pracovní dny 06.00 – 18:00 hod
WWW stránky	[redacted]
E-mail	[redacted]
Telefon	[redacted]

1.2 Hlášení, proces jeho přijetí a zpracování

Hlášení může být podáno Zadavatelem nebo Dodavatelem a reprezentuje dotaz, identifikaci vady či požadavek, jež je třeba dále zpracovat. Hlášení je identifikováno a zapsáno v interním systému Dodavatele pod jednoznačným identifikátorem a je reprezentováno Zadavateli přes aplikaci HelpDesk. Základní charakteristika hlášení je definována jeho typem.

Typy hlášení jsou:

- DOTAZ
- VADA
- POŽADAVEK

Proces přijetí a zpracování hlášení obsahuje:

1. Přijetí Hlášení: okamžikem Přijetí Hlášení se rozumí čas, kdy je Hlášení Dodavatelem přiřazen jednoznačný identifikátor. Ten Dodavatel přidělí bez ohledu na to, zda je hlášení úplné. U neúplných hlášení může Dodavatel požadovat od Zadavatele popis kroků vedoucích k vysvětlení problému popsaného v hlášení tak, aby bylo možné nasimulovat problém nebo jej alespoň

identifikovat - např. kopie obrazovek systému, popis chybových hlášek, podmínky výskytu problému, použitá vstupní data, atd. Pokud je Hlášení podáno v Provozní době, je Přijetí provedeno bezprostředně po nahlášení. Pokud je Hlášení podáno mimo Provozní dobu, zajistí Dodavatel Přijetí Hlášení bezprostředně po zahájení nejbližší Provozní doby.

2. Klasifikace Hlášení a prvotní podpora – posouzení typu hlášení, stupně závažnosti, případně doporučení náhradního řešení

3. Řešení hlášení – proces vedoucí k vyřešení hlášení

4. Vyřešení hlášení – zodpovězení DOTAZU, vyřešení vady (uvedení Systému do souladu s Dokumentací, realizace funkčního náhradního řešení), zapracování změnového požadavku a jeho nasazení do Systému

5. Uzavření hlášení – vyjádření Zadavatele k vyřešenému hlášení ve lhůtě 5 pracovních dnů nebo uplynutím této lhůty, pokud se Zadavatel k vyřešenému hlášení nevyjádří. Dodavatel a Zadavatel se mohou v konkrétních případech dohodnout na jiné lhůtě.

Procesy práce s hlášeními zohledňují parametry a rozsah záručního servisu, včetně klasifikace chyb a SLA, dle kapitoly 3.3.2 Zadávací dokumentace. Práce se zákaznickými hlášeními bude odpovídat dosavadním zavedeným postupům Dodavatele, včetně postupů krizové komunikace.

1.3 Informační systém HelpDesk

Nahlášení požadavku/vady/dotazu na službu Helpdesk bude možné uskutečnit v režimu 24/7 prostřednictvím IS HelpDesk Dodavatele nebo prostřednictvím interního ServiceDesku Zadavatele - SDM. Oprávněná osoba Zadavatele může Hlášení učinit prostřednictvím webové části HelpDesku, ale v provozní době rovněž emailem či telefonicky na výše uvedené helpdeskové kontakty. Hlášení bude zapsáno do systému HelpDesk a bude mu přiděleno unikátní číselné označení, které si ponese po celou dobu jeho řešení.

Hlášení může podat a v rámci jeho řešení participovat jakákoliv oprávněná osoba zadavatele či definovaní zástupci třetích stran (subdodavatelé Zadavatele). Počet oprávněných uživatelů je možné změnit na základě autorizačního procesu definovaného ve smlouvě (validovaný seznam oprávněných osob).

IS HelpDesk potvrdí příjem Hlášení Zadavateli notifikačním e-mailem, který bude obsahovat zvalidované parametry hlášení (např. závažnost, prioritu, dotčený systém/služba atd.) a dle povahy incidentu též oznámí způsob řešení a předpokládaný čas vyřešení.

Webová aplikace HelpDesk byla vyvinuta společností CCA Group a.s. a je navázána na interní informační systém pro administraci zákaznických požadavků a řízení výroby. Pro zákazníka bude přístupná na webových stránkách https://hotline.cca.cz.

Aplikace HelpDesk byla navržena podle best practices procesů ITIL a kombinuje uživatelský komfort na straně zákazníka a kompletní podporu procesů service desku na straně dodavatele služby. Aplikaci momentálně využívá více jak 200 zákazníků CCA Group a.s., což činí zhruba 1100 oprávněných uživatelů.

Základní funkce aplikace Helpdesk jsou:

- Řízený přístup k hlášením z pozice zákazníka, CCA i dalších dodavatelů ICT služeb – zřízení uživatelského účtu s možností individuálního nastavení včetně mailových notifikací

- Možnost zadávat nová hlášení (vady, požadavky, dotazy) a to buď přímo přes webovou aplikaci, e-mailem, telefonicky či automaticky alarmem z monitorovacích zařízení. K hlášení je možné přiložit přílohy.

- Detail hlášení zobrazuje podrobné informace o řešení hlášení včetně termínu zadání, termínu do kterého má být vyřešeno, prioritizaci, aktuálním stavu a všech komunikacích nad hlášením vedených
- Informování zúčastněních stran o řešení Hlášení prostřednictvím automatických notifikací
- Filtrování a vyhledávání v Hlášeních dle zadaných kritérií
- Poskytování informací a oznámení o právě probíhajících událostech, které se vztahují k práci se systémy zákazníka – odstávky, omezení funkčnosti, informace pro uživatele
- Úložiště dokumentů vztahující se k provozovaným systémům – nápovědy, příručky, distribuční protokoly

1.4 Zavedení služby a úvodní nastavení systému HelpDesk

Po podpisu smlouvy budou neprodleně zahájeny práce na aktualizaci nastavení nabízených služeb v systému HelpDesk. To obnáší zejména:

- Vydefinování podporovaných systémů/služeb včetně identifikace návazných systémů a služeb
- Stanovení druhů hlášení a procesů jejich řešení (stavy hlášení)
- Stanovení kategorií priorit a dopad prioritizace na procesy/stavy v hlášení (dle klasifikace uvedené v ZD kapitole 3.32 případně dalších požadovaných)
- Nastavení lhůt řešení pro všechny druhy hlášení (měřitelné parametry SLA odpovídající požadavkům dle kapitoly 3.3.2 ZD)
- Přiřazení oprávněných řešitelů k hlášením a způsob notifikací

1.5 Automatizované propojení na SD zadavatele

V souladu s požadavky zadavatele, pro posílení a zrychlení spolupráce mezi Zadavatelem a Dodavatelem služeb, je již v současné době realizováno propojení helpdeskového systému CCA Group a.s. s SDM systémem ČUZK. Toto propojení bude provozováno i nadále po podpisu smlouvy na plnění servisu v letech 2021-2025.

Prostřednictvím automatizovaného propojení výše uvedených systémů Dodavatel plně realizuje požadavky uvedené v kapitole 3.3.2 Zadávací dokumentace a přílohy č. 8 této zadávací dokumentace.

Předmětem propojení je pokrytí těchto základních procesů:

- Přenos vytvořeného hlášení z SDM Zadavatele do Helpdesku CCA Group a.s. na základě inicializačního procesu
- Přenos dodatečných informací a příloh připojených v SDM Zadavatele k vytvořenému hlášení v Helpdesku CCA Group a.s.
- Přenos informací z Helpdesku CCA Group a.s. do SDM Zadavatele (ID hlášení dodavatele, dodávka, CR, stav, komentář a další)
- Informace a reakce o stavech hlášení (Vyjádření ČUZK, Odmítnutí řešení, Ukončení řešení, Změna priority či kategorie)

Propojení SDM systémů je realizováno za použití webových služeb na technologii SOAP.

Metodika interního testování dodávek DMS

1 Popis metodiky interního testování pro dodávky DMS

Procesy interního testování v CCA Group a.s. popisuje dokument Metodika testování (soubor S018_M05_Testovani.pdf), jež je přílohou nabídky. Jedná se o standardizovaný dokument politiky jakosti CCA Group a.s., který je závazný pro všechny pracovníky Dodavatele.

Metodika vysvětluje pojmy používané v procesu testování, definuje činnosti Test analytika a Testera, popisuje cíle, rozsah, strategie a způsoby testování, včetně postupů pro evidenci testovacích činností ve výrobním informačním systému CCA Group a.s. Jedná se o komplexní dokument postihující celý cyklus kontroly jakosti výroby SW od raných fází po implementaci. Metodika testování byla vytvořena dle mezinárodně platných metodik ISTQB a norem IEEE 829–2008 BS 7925-1 a BS 7925-2.

Při vývoji software používá CCA Group a.s. standardizovaný V-Model (Sequence Development Model), přičemž testování je v tomto modelu součástí všech fází návrhu a vývoje. Pro každou část výroby produktu existuje ekvivalentní testovací proces, který přináší okamžitou zpětnou vazbu, čímž zajišťuje včasné odhalení chyb, snížení nákladů na jejich korekci a zpřesnění plnění zákaznických požadavků.

Základní cíle testování jsou nacházení a prevence SW chyb, zvyšování důvěry v úroveň kvality a poskytování informací vývojovému týmu i dalším zainteresovaným stranám. Z tohoto důvodu je testování v CCA Group integrální částí výrobního procesu. Přestože je testovací tým nezávislý na vývojářích, pro reporting a sdílení informací jsou používány interní informační systémy Dodavatele. Tester má tak k dispozici veškerou potřebnou vývojovou dokumentaci a zároveň odhalené chyby jsou zadávány přímo k opravě formou úkolů v interním výrobním systému. Testeři se účastní či sami iniciují rewiev (přezkoumání, revize) na úrovni jednotlivců či celého týmu. Tento přístup garantuje rychlý přenos informací a jejich sdílení na formální i neformální bázi.

Způsob a metodika vývoje

Způsob a metodika vývoje je řízena interní metodikou **S018 – Projektový zákon**. Tato metodika zahrnuje posloupnost jednotlivých dílčích fází:

Směrnice	S018 – Projektový zákon
Dílčí fáze	Fáze zahájení
Účel dokumentu	Definice jednotlivých kroků v rámci fáze zahájení

Cílem fáze je připravit vlastní zahájení projektu. Fáze zahájení projektu je tvořena následujícími kroky:

- **Projektový záměr**
  Projektový záměr vzniká na základě požadavku na vyhodnocení realizovatelnosti projektu. Odpovídá na otázku, zda je možné a rozumné navržený projekt – realizovat

- **Příprava startovní dokumentace**
  Příprava startovní dokumentace je prvním krokem při realizaci projektu. Navazuje na rozhodnutí o realizaci projektu. Zásadním výstupem je zpracování „Pověření o řízení projektu“

- **Specifikace účelu a cílů projektu**
  Cílem tohoto kroku je zajistit správnou specifikaci účelu a cílů projektu, z níž se vychází pro analýzu a projekt

Směrnice	S018 – Projektový zákon
Dílčí fáze	Fáze příprava
Účel dokumentu	Definice jednotlivých kroků v rámci fáze příprava

Cílem fáze je připravit veškeré nutné výstupy spojené se správnou specifikací projektu a zadáním nutným pro následující konstrukční fázi. Fáze zahájení projektu je tvořena následujícími kroky:

- Specifikace požadavků
- Studie proveditelnosti
- Analýza a návrh pro zákazníka
- Posouzení ANZ v ZP
- Analýza a návrh pro VV
- Architektura SW
- Test analýza –plán
- Test analýza – testovací scénáře

Směrnice	S018 – Projektový zákon
Dílčí fáze	Fáze konstrukce
Účel dokumentu	Definice jednotlivých kroků v rámci fáze konstrukce

Cílem fáze je vytvořit a ověřit sw produkt podle zpracované dokumentace. Dále pak připravit projekt zavedení u zákazníka. Fáze zahájení projektu je tvořena následujícími kroky:

- Programování
- Ověření v AP
- Projekt zavedení u zákazníka
- Testování v ZP
- Správa technického prostředí a model nasazení

Směrnice	S018 – Projektový zákon
Dílčí fáze	Fáze nasazení
Účel dokumentu	Definice jednotlivých kroků v rámci fáze nasazení

Cílem fáze je zavést vytvořený produkt do užívání u zákazníka a následně zajistit předání a uzavření projektu. Fáze zahájení projektu je tvořena následujícími kroky:

- Instalace
- Převzetí zákazníkem do ověřovacího provozu
- Výroba dokumentace k produktu
- Školení
- Ověření pilotními uživateli
- Plošné nasazení
- Předání do rutinního provozu
- Uzavření projektu

Pokud je zpracován dokument Projekt zavedení u zákazníka probíhá celý proces zavedení podle tohoto dokumentu.

Celý projekt vývoje a nasazení řídí vedoucí projektu. **Cílem je řídit projekt tak, aby byl dokončen OTIFOB (on time, in full, on budged) ke spokojenosti zákazníka**. Fáze řízení projektu začíná jeho zahájením a končí uzavřením.
V průběhu řízení projektu vedoucí projektu organizuje vykonávání metodických kroků definovaných v jednotlivých fázích v souladu s potřebami projektu a metodickými nařízeními. K úkolování členů týmu používá systém ISZA, řízení rozpočtu systém IMIS a ke sdílení informací IDMS a firemní portál.

Zodpovědnosti vedoucího projektu:

- **Dokončení projektu OTIFOB**
- **Řízení projektu**
- Vedoucí projektu zodpovídá za správné navržení cash-flow projektu (projekt není nikde v průběhu dotován z jiných zdrojů). V případě potřeby si výjimky nechá schválit vedením společnosti
- Vedoucí projektu zodpovídá za dodržování platných interních směrnic a metodik kvality v rámci činností, které jsou předmětem projektu.
- Vedoucí projektu kontroluje výstupy, zejména dokumentaci z pohledu metodického a úplnosti a to nezávisle na akceptantech kroků. Pokud se Vedoucí projektu domnívá, že není dostatečně znalý věci, může si vyžádat posudek příslušného znalce, např. vedoucího metodiky nebo ředitele úseku.
- Vedoucí projektu zodpovídá za stanovení akceptačních kritérií se zákazníkem a předání díla dle smluvní dokumentace
- Vedoucí projektu zodpovídá, za vedení úkolů v ISZA
- Vedoucí projektu zodpovídá za vytvoření a aktualizaci vyjmenovaných příloh k servisním smlouvám.

Základní činnosti řízení projektu:

- Řízení projektu na cíl
- Řízení lidských zdrojů
- Řízení komunikace
- Řízení rizik
- Řízení smluvních vztahů
- Řízení nákladů a financí
- Řízení subdodávek
- Schvalování výkazů prací
- Vedení dokumentace
- Změnové řízení

Vedení dokumentace – projektová kancelář

1 Popis základních principů a způsobu vedení dokumentace projektových výstupů a vedení projektové kanceláře

Firma CCA vyrábí systémy v souladu s běžnými standardy pro tvorbu software. Při výrobě software vychází ze standardních metodik (zejména Unified process), které má přizpůsobené pro vlastní potřebu. Pro veškerou dokumentaci má připravenou řadu šablon s návody na jejich použití. Základní směrnicí pro tvorbu software je tzv. Projektový zákon, který předepisuje postupy řízení projektu spolu s výrobními procesy. Základním cílem činností předepsaných činností Projektového zákona je uspokojení požadavků zákazníka. Prostředkem k dosažení tohoto cíle je kromě samotného vývoje software řádná dokumentace projektu, důraz na otestování a finální akceptace zákazníkem.

CCA je držitelem ISO certifikátů ISO 9001:2015, ISO/IEC 27001:2013, ISO/IEC 20000-1:2018 pro oblasti konzultace, zpracování analýz a projektu, vývoj a údržba software, implementace a poprodejní servis v oblasti komplexních řešení informačních technologií a systémové integrace.

Firma CCA průběžně dokumentuje všechny fáze výroby od prvotního seznam požadavků a analýzy, přes technickou dokumentaci vyvíjeného systému až po uživatelskou příručku. Dodávka vybrané části dokumentace je vždy předmětem dohody se zákazníkem. V dalších kapitolách je ukázáno, jak použití metod CCA naplňuje požadavky Zadavatele.

1.1 Postup tvorby a dokumentace SW v prostředí CCA Group a.s.

Veškeré výstupy, které v projektech vznikají jsou definovány metodikami a vlastní zpracování výstupů je podpořeno používanými interními systémy. Práce na projektech je zadávána prostřednictvím tzv. plánu projektu. Plán projektu rozděluje činnosti při tvorbě projektu do fází a iterací. Přitom předepisuje **povinné a volitelné výstupy, které během realizace vznikají.** Výstupem je zpravidla dokumentace nebo program.

Plán projektu dále obsahuje úkoly pro konkrétní pracovníky, kteří předepsané výstupy vytvářejí. Součástí metodologie práce s plánem projektu jsou postupy pro akceptaci a testování výstupů včetně kritérií akceptace.

Plán projektu

Použít šablonu | Stav plánu projektu | E | Historie | Stornuj PP

	SK	Krok	Vlastní název kroku	Termín zahájení Plán	Termín zahájení Skutečnost	Termín doručení Plán	Termín doručení Skutečnost	Termín akceptace Plán	Termín akceptace Skutečnost	Řeš.	Akc.
Úk.	E	Detailní návrh pro zákazníka		26.07.2014	25.07.2014	05.05.2015	04.05.2015	05.05.2015	04.05.2015	VAT	VAT
Úk.	E	Instalace	v CCA	24.07.2014	23.07.2014	05.05.2015	04.05.2015	05.05.2015	04.05.2015	VAT	VAT
Úk.	E	Instalace	v ČÚZK	02.05.2014	01.05.2014	05.05.2015	04.05.2015	05.05.2015	04.05.2015	VAT	VAT
Úk.	E	Posouzení ANZ v ZP		12.05.2014	12.05.2014	22.05.2014	21.05.2014	12.07.2014	11.07.2014	GAE	VAT
Úk.	E	ANV - vazba na externí IS		26.06.2014	25.06.2014	29.04.2015	28.04.2015	30.04.2015	29.04.2015	FAJ	VAT
Úk.	E	ANV - hromadný vstup dokume		17.06.2014	16.06.2014	29.04.2015	28.04.2015	30.04.2015	29.04.2015	FAJ	VAT
Úk.	E	ANV - III. oblast		05.07.2014	04.07.2014	29.04.2015	28.04.2015	30.04.2015	29.04.2015	FAJ	VAT
Úk.	E	ANV - skartační řízení		18.06.2014	17.06.2014	29.04.2015	28.04.2015	30.04.2015	29.04.2015	FAJ	VAT
Úk.	E	ANV - vazba na OB-A		17.06.2014	16.06.2014	29.04.2015	28.04.2015	30.04.2015	29.04.2015	FAJ	VAT
Úk.	E	ANV - přístupová práva		22.08.2014	21.08.2014	29.04.2015	28.04.2015	30.04.2015	29.04.2015	FAJ	VAT
Úk.	E	PRG - vazba na externí IS		25.06.2014	24.06.2014	21.05.2015	20.05.2015	11.08.2015	10.08.2015	HRO	VAT
Úk.	E	PRG - hromadný vstup dokume		31.07.2014	30.07.2014	05.05.2015	04.05.2015	05.05.2015	04.05.2015	FAJ	VAT
Úk.	E	PRG - skartační řízení		14.10.2014	13.10.2014	21.05.2015	20.05.2015	11.08.2015	10.08.2015	HRO	VAT
Úk.	E	PRG - vazba na OB-A		14.08.2014	13.08.2014	21.05.2015	20.05.2015	11.08.2015	10.08.2015	HRO	VAT

Obrázek: Plán projektu

Pro všechny typy dokumentů, které vznikají při plnění úkolů plánu projektu, jsou definovány šablony. Šablony zajišťují jednotnou formu dokumentace a umožňují pracovníkovi soustředit se na obsah tvořeného

dokumentu. Metodologie CCA v současnosti eviduje cca 60 šablon. Část šablon pokrývá řídící činnosti projektu a jsou určeny pro project managera, část se týká výroby a část zavedení hotového produktu do produkce.

Vybrané výrobní šablony jsou uvedeny v tabulce:

Šablona	Zkratka	Popis
S018_M02_Š02_Seznam požadavků	POZ	Seznam požadavků na vyráběný produkt. Dokument je ve formě excelu a slouží zejména pro řízení výroby a jednání se zákazníkem o stavu projektu
S018_M03_Š03_Plán testování	TPL	Uvádí strategii testování a plán testů
S018_M02_Š08a_Analýza a návrh pro zákazníka	ANZ	Dokument rozpracovává požadavky do popisu cílového řešení tak, aby se zákazník i dodavatel shodli, jak bude cílový produkt vypadat a jaká bude jeho funkčnost
S018_M02_Š05_Analýza a návrh VV	ANV	Podrobná technická dokumentace systému. Obsahuje popis uživatelského rozhraní, všech procesů, funkcí, komunikací, a další.
S018_M03_Š07_Datový_model	DM	Doplněk ANV. Podle rozsahu projektu může být uveden jako samostatný dokument nebo může být součástí dokumentu ANV
S018_M02_Š06_SW_Architektura	ASW	Dokumentace hardwarové a softwarové architektury systému.
S018_M03_Š04_Testovací scénář	TSC	CCA eviduje jednotlivé testovací scénáře a kroky testů v interním systému ISZA (Informační systém zákaznické administrace). Testovací scénáře lze exportovat do formy dané šablonou nebo do formátu vhodného pro přenos do systému třetí strany
S018_M04_Š14_Distribuce řešení	DRES	Popis instalace systému nebo instalace jeho nové verze

Šablony a struktura dokumentace jsou vždy na začátku projektu přizpůsobeny potřebám, zvykům a názvosloví zákazníka.

1.2 Ukládání projektové dokumentace

Kapitola navazuje na požadavky kapitoly 4.3.1. Dokumentace dokumentu Zadávací dokumentace DMS.

Veškerá dokumentace je vedená v interním dokumentovém systému IDMS. Každý projekt má v systému vyhrazený prostor. Tento prostor odpovídá požadavkům na projektovou kancelář ze zadávací dokumentace. Prostor je možné zpřístupnit zákazníkovi.

Požadavek	Způsob splnění
Vzdálený přístup pro zástupce Zadavatele prostřednictvím sítě internet, včetně možnosti online editace uložených dokumentů pomocí klientských aplikací MS Office.	IDMS pracuje na webové platformě. Součástí platformy je i omezení uživatelských práv k dokumentům. Zpřístupnění zástupcům Zadavatele je možné, je možná i vzdálená editace dokumentů prostřednictvím nástrojů MS Office.
Verzování dokumentů.	IDMS podporuje verzování dokumentů na dvou úrovních. Při editaci vyžaduje rezervaci dokumentu. Při ukončení rezervace uživatel vytváří menší verzi. Když je dokument dokončený, zvýší uživatel číslo na první úrovni.

Fultextové vyhledávání.	Ano, je podporované
Různé kategorie dokumentů z hlediska bezpečnosti (standardní, důvěrné, …) a možnost řízení přístupu k těmto kategoriím.	Řízení přístupů k dokumentům z hlediska bezpečnosti je zpravidla řízeno členěním dokumentů do složek podle stupně bezpečnosti a nastavením přístupů na tyto složky. Také je možné nastavení přístupů na konkrétní dokument.
Struktura s rozdělením dokumentů podle logických kategorií (zápis z jednání, žádosti o změnu, dokumentace, …).	Dokumenty lze členit do složek podle potřeby. Dokumenty lze také kategorizovat pomocí metadat a podle těchto metadat je také vyhledávat/zobrazovat
Automatické číslování nových dokumentů v kategoriích podle předchozího požadavku.	V současnosti Dodavatel tuto funkčnost nepoužívá, dokumenty jsou číslovány ručně podle vnitřní metodologie. Nicméně knihovna tuto funkčnost umožňuje.
Logování a audit přístupů do PK k jednotlivým dokumentům.	Systém audituje veškeré změny dokumentu včetně údaje o pracovníkovi, který změny prováděl. Systém dále nabízí široké možnosti logování, je možné sledovat i jednotlivá otevření dokumentu
Možnost rezervace (zamluvení) nových dokumentů podle jednotlivých logických kategorií, systém přidělí číslo v čase rezervace.	Rezervace dokumentu je podmínkou pro provádění změn
Uložení různého typu dokumentů (Word, Excel, MS Project, ZIP, RAR, …).	Dokumenty sady MS Office jsou standardně dovolené, ostatní lze jednoduše zapnout podle požadavků zákazníka
Možnost uložení jen dokumentů schválených oboustranně a dle schválené jmenné konvence	Tuto funkcionalitu systém IDMS nemá, lze ji ovšem doplnit. Lze ji zapracovat i tak, že dovolí uložit dokument, ale bude informovat správce a ten zjedná nápravu nebo dovolí výjimku
Export PK na filesystém se zachováním všech verzí dokumentu.	Export knihovny projektové formuláře včetně všech verzí dokumentů na filesystém je možný. Vyexportovaný soubor je v proprietárním formátu microsoft. Poslední verze dokumentů lze jednoduše exportovat do běžné struktury složek filesystému. Podle potřeby můžeme dopracovat export, který bude exportovat také historické verze dokumentů vždy s číslem verze doplněným v názvu souboru
Definice povolených masek jmen dokumentů.	Tuto funkcionalitu lze doplnit. Je předpokladem pro požadavek možnosti uložení dokumentů podle jmenné konvence.

Programátorská dokumentace:

Kapitola navazuje na požadavky kapitoly 4.3.1.1 Programátorská dokumentace dokumentu Zadávací dokumentace DMS.

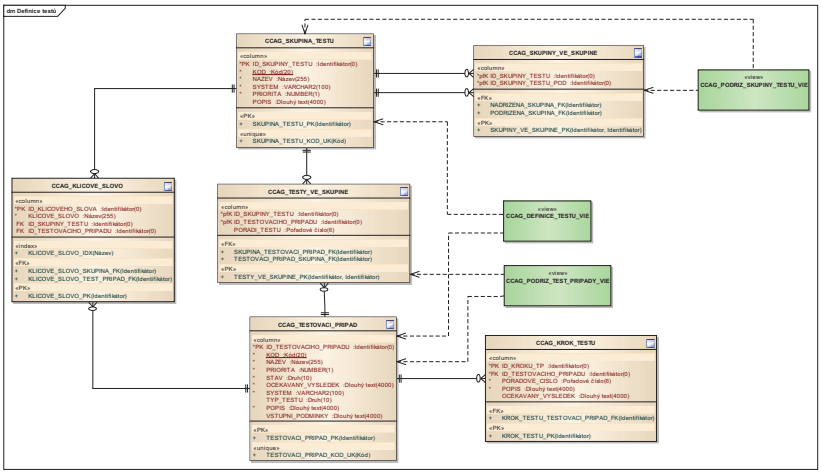
Programátoři jsou povinni dokumentovat kód formou komentářů. Kromě toho vzniká sada dokumentace, která popisuje procesy a funkcionalitu systému. Dokumentace primárně vzniká v nástroji Enterprise Architect a je generována do formy dokumentů ANV, resp. ASW. Tyto popisy jsou v udržovány aktuální, vetší část jich vzniká ještě před vlastním programováním a slouží jako jeho zadání.

Databázové objekty

Datový model obsahuje informace o strukturách, kam jsou ukládána data aplikace. Primárně obsahuje:

- Schématické znázornění modelu
- Seznam logických datových typů
- Název entity/tabulky/pohledu
- Popis entity/tabulky/pohledu
- Seznam atributů entity/sloupců tabulky
  - Název atributu
  - Datový typ
  - Povinnost
  - Velikost
  - Popis
- Seznam klíčů tabulky (primární/unikátní, cizí klíče včetně logických)
- Validační podmínky (check constraint)

Příklad diagramu datového modelu:



Příklad popisu tabulky:

CCAG_KROK_TESTU «table»
Krok definice testovacího případu.
Sloupce

PK	Název	Typ	Pov.	Unique	Len	Prec	Scale	Init	Poznámky
True	*ID_KROKU_TP*	*Identifikátor*	*True*	*False*	*0*	*0*	*0*		*Interní identifikátor kroku testu generovaný ze sekvence.*
False	*ID_TESTOVACIHO_PRIPADU*	*Identifikátor*	*True*	*False*	*0*	*0*	*0*		*Odkaz na testovací případ, kam krok patří*

False	*PORADOVE_CISLO*	*Pořadové číslo*	*True*	*False*	*0*	*6*	*0*		*Pořadové číslo kroku v rámci testovacího případu.*
False	*POPIS*	*Dlouhý text*	*True*	*False*	*4000*	*0*	*0*		*Detailní popis kroku - co přesně tester dělá, kde klikne, atd.*
False	*OCEKAVANY_VYSLEDEK*	*Dlouhý text*	*False*	*False*	*4000*	*0*	*0*		*Očekávaný výsledek provedení kroku.*

Constrainty

Název	***Typ***	***Sloupec***	***Poznámky***
KROK_TESTU_TESTOVACI_PRIPAD_FK	*Public*	*ID_TESTOVACIHO_PRIPADU*	
KROK_TESTU_PK	*Public*	*ID_KROKU_TP*	

Relace

Sloupec	*Vazby*	
	0.. *1*	*CCAG_KROK_TESTU.* *Výsledek kroku.*
	0.. *1*	*CCAG_KROK_TESTU.KROK_TESTU_TESTOVACI_PRIPAD_FK* *CCAG_TESTOVACI_PRIPAD.PK_CCAG_TESTOVACI_PRIPAD*

Aplikační moduly

Aplikační moduly jsou popsány formou dokumentů ANV. Podle velikosti projektu mohou být hierarchicky členěny. Na nejvyšší úrovni je popsán systém jako celek a jeho členění na nižší komponenty včetně popisu jejich odpovědnosti. Takto je popis členěn až na úroveň jednotlivých programových modulů/funkcí.

Dokumentace programového modulu obsahuje

- Procesy, kterých se modul účastní
- Část datového modelu, se kterým modul pracuje (může být formou odkazu do samostatného dokumentu datového modelu)
- Zařazení modulu do menu aplikace
- Případy užití, které modul realizuje
- Vzhled a popis uživatelského rozhraní
- Popis napojení uživatelského rozhraní na datové struktury včetně validačních podmínek
- Seznam rolí, jejichž uživatelé jsou oprávněni aplikační modul používat.

Model komponent

Popis komponent je součástí dokumentace aplikačních modulů v dokumentech ANV na vyšších úrovních hierarchie. Popis komponent se také objevuje v dokumentu ASW (architektura systému). Obsahuje komponentový model, člení systém nebo jeho část do menších celků. Komponenty jsou dokumentovány

- Názvem
- Jednoznačným kódem
- Popisem

Součástí popisu komponent je popis jejich rozhraní.

Popis komunikací a aplikačních rozhraní

Pokud je součástí systému komunikace v rámci systému nebo s jiným systémem, je samostatně dokumentována. Dokumentace obsahuje dynamickou část (proces komunikace, tedy jak na sebe navazují volání funkcí, případně jak si oba aktéři komunikace potvrzují přijetí, apod.) a statickou část, tedy popis datových struktur komunikace ve formě class diagramů.

Dokumentace obsahuje

- Proces komunikace, pokud na sebe například navazují potvrzující zprávy
- Seznam a popis funkcí komunikačního rozhraní
- Datové struktury předávané v rozhraní
- Návratové kódy volání
- Zabezpečení komunikací
- Popis pravidel verzování komunikačního rozhraní

Popis procesů

Procesy jsou v dokumentaci popisovány na několika úrovních – na úrovni business procesů, zejména pro popis toků dat u zákazníka nebo i mezi zákazníkem a třetími subjekty, a na úrovni algoritmů jednotlivých funkcí. Pro popis business procesů je používána BPMN notace, algoritmů jsou popisovány prostřednictvím diagramů aktivit a sekvenčních diagramů.

Popis nasazení – Deployment model

Popis nasazení dokumentuje skutečné nasazení softwarových komponent aplikace na hardware. Součástí popisu jsou požadované nároky na hardware. Deployment model je uveden v dokumentu ASW (Architektura systému).

Popis tříd

Popis tříd se používá zejména pro podrobnou dokumentaci rozhraní modulů, a to vnitřních i vnějších. Pro popis tříd se používá běžný Class diagram, pro podrobnější vysvětlení funkčních vztahů a volání tříd pak Sekvenční diagram. U tříd a interface evidujeme

- Název třídy/interface včetně zařazení ve struktuře package/namespace
- Popis třídy/rozhraní
- Seznam atributů tříd
    - Název atributu
    - Datový typ
    - Viditelnost atributu (public, private, …)
    - Popis atributu
- Seznam metod a konstruktorů/destruktorů
    - Název metody
    - Popis – co metoda dělá, případně co je jejím výstupem
    - Parametry metody včetně datových typů
    - Typ návratové hodnoty metody (význam hodnoty je uveden v popisu metody)

Pro významné třídy bude navíc uveden příklad jejich volání. Tento postup je běžný zejména u tříd, které jsou součástí komunikace se systémy třetích stran.

Údržba provozní dokumentace:

Kapitola navazuje na požadavky kapitoly 4.3.1.2 Provozní dokumentace dokumentu Zadávací dokumentace DMS.

Dodavatel se zavazuje udržovat provozní dokumentaci systému aktuální. Přednostně zajistí aktualizaci dokumentů podle zadávací dokumentace

- DL005DMS2 Uživatelská dokumentace DMS
- DL006DMS2 Řízení přístupu
- DL007DMS2 Prostředí DMS
- DL008DMS2 Uživatelská dokumentace DMS – administrátor
- DL009DMS2 Rozhraní WS DMS
- DL010DMS2 Technický popis infrastruktury DMS
- DL011DMS2 Zátěžový test
- DL017SDMS2 Konfigurace DMS

- OW002DMS2 Metadata k migraci
- OW003DMS2 Přehled metadat v DMS
- OW004DMS2 Mapování metadat k typům dokumentů
- PS002DMS2_Popis_importu_dat

Všechny tyto dokumenty zapadají do metodologie tvorby projektové dokumentace Dodavatele. Dokumentace bude udržována v souladu s požadavky Zadavatele (přehled činností administrátora, apod.).

Instalační příručky:

Kapitola navazuje na požadavky kapitoly 4.3.1.3 Instalační příručky DMS dokumentu Zadávací dokumentace DMS.

Dodavatel podle metodiky tvoří instalační příručky systémů, jak pro prvotní instalaci celého systému, tak pro distribuce nových verzí. Instalační příručka standardně obsahuje

- Přípravné kroky instalace
- Postup instalace komponent podle jejich závislostí
- Podrobný popis instalace jednotlivých komponent
- Popis nastavení prostředí, které je nutné v rámci instalace provést (typicky nastavení proměnných prostředí, parametrů systému, napojení na databázi, apod.)

Naplnění požadavků zadávací dokumentace na instalační příručku ukazují následující body:

a) Členění po jednotlivých logických celcích DMS a po vrstvách TI (DB, aplikační, klientská, …) – výše uvedenými komponentami v částech instalační příručky se rozumí také databázový server, aplikační server, …
b) Specifikace požadavků na infrastrukturu a SW – Tato specifikace je součástí dokumentu Správa technického prostředí, potažmo Architektura systému. Pokud má instalace specifické požadavky na infrastrukturu a SW vybavení, jsou uvedené v těchto dokumentech a také v instalační příručce
c) Nemusí popisovat obecnou instalaci OS a SW (Oracle produkty, případně další běžné produkty) – míra podrobnosti popisu instalační příručky je vždy předmětem dohody se zákazníkem.
V každém případě součástí instalační příručky jsou nastavení operačního systému nebo dalších používaných produktů, které jsou specifické pro daný systém (systémové parametry, připojení k databázi z aplikačního serveru, nutné síťové prostupy, nastavení zabezpečení, …). Dodavatel se dále zavazuje poskytnout potřebnou součinnost při popisu obecných instalací.
d) Popis všech kroků pro úspěšnou instalaci komponent DMS (vytvoření DB schématu, vytvoření tablespace, nahrání DB objektů, zapojení replikací mezi DB, j2ee serverů, deploy Java aplikací, uložení certifikátů a klíčů, apod.) – všechny tyto komponenty a nastavení jsou vždy popsány v instalační příručce v popisu instalace komponent a v popisu nastavení prostředí.
e) Popis veškeré aktuální konfigurace systému – popis je součástí instalační příručky. Pro rozsáhlé systémy je instalační příručka členěna do více souborů ve struktuře dohodnuté se zákazníkem. Struktura je uvedena v příloze instalační příručky. Takto mohou být součástí příručky konfigurační soubory a další nastavení.
f) Aktualizace při změnách konfigurace i při nových verzích systémů DMS – Instalační příručka je součástí každé distribuce nové verze systému. Kromě samotného popisu způsobu nasazení nové verze obsahuje změny nastavení systému, které je nutné během instalace provést.
g) Datová struktura DMS musí být primárně vedena v programátorské dokumentaci – datový model je součástí projektové dokumentace. Metodologie Dodavatele vyžaduje povinné komentování tabulek a sloupců v databázi. Podle požadavku Zadavatele přidáme do komentáře tabulky povinné označení verze.
h) Přehled všech možností konfigurace systému – nastavení systému je nedílnou součástí dokumentace. Vždy je uvedeno označení parametru/nastavení, způsob jeho nastavení (kde se nastavuje a jak, případně kde je nastavení uloženo) a dopad tohoto nastavení, tedy co lze nastavit a jak se toto nastavení projeví v systému. Dále je uvedeno, jestli se změna nastavení projeví hned nebo později (po opětovném přihlášení uživatele, po restartu komponenty, po restartu systému).

Součástí instalační příručky je protokol se seznamem změnových požadavků v dodané verzi a způsobem jejich realizace. V protokolu jsou uvedeny také změny nastavení a požadavky, které změny vyvolaly.

i) Přehled všech modulů aplikací DMS (i „nevizuální“ moduly) – dokumentace popisuje všechny moduly, tedy i ty bez uživatelského pozadí, která vykonávají činnost na pozadí. Metodologie dodavatele požaduje důkladné zaznamenávání činnosti těchto modulů. Seznam zpráv zaznamenávaných těmito moduly je součástí dokumentace.
   Součástí instalační příručky je protokol se seznamem změnových požadavků v dodané verzi a způsobem jejich realizace. V protokolu jsou uvedeny také změny modulů a požadavky, které změny vyvolaly.
j) Přehled a popis databázových jobů a scheduled task vytvořených či vyžadovaných systémy DMS – Úlohy, které běží na pozadí, jsou dokumentovány stejně jako ostatní moduly aplikace. Vždy je uvedeno
   - Název a kód úlohy
   - Popis úlohy
   - V jakém prostředí úloha pracuje (dB job, úloha operačního systému, timer aplikačního serveru, …)
   - Četnost spouštění, případně událost, která ji vyvolá
   - Způsob zaznamenávání průběhu úlohy včetně popisu, jak průběh zobrazit
   - Popis, jaký vliv má na úlohu restart systému. V instalační příručce je explicitně uvedeno, jestli je nutné při instalaci nové verze úlohy vypínat nebo ne
k) Dokumentace vazeb DMS na okolní IS – Dokumentace okolí bude součástí dokumentace. Pro zobrazení komunikací Dodavatel používá diagram komponent nebo podobný komunikační diagram. Diagramy jsou vždy doplněny popisem. Každé rozhraní bude podrobně popsáno (viz Popis komunikací a aplikačních rozhraní výše)
l) Další nastavení a činnosti systémů DMS
   - zakládání speciálních uživatelů
   - nastavování práv a řízení přístupu
   - používání certifikátů (bezpečné uložení certifikátů)

   Všechna další nastavení a činnosti včetně uvedených budou součástí instalační příručky. Dodavatel vždy věnuje zvýšenou pozornost zabezpečení systému a komunikací, což se bez podrobné dokumentace nastavení neobejde.
m) Popis logování systému – Způsob logování jednotlivých komponent je součástí jejich popisu. Administrátorské nastavení systému logování je součástí instalační příručky. Dokumentace obsahuje
   - Umístění logů na všech úrovních systému (databáze, aplikační server, operační systém, klientská stanice)
   - Způsob nastavení systému logování (umístění souborů, rotace log souborů, správa logu v databázi)
   - Způsob nastavení úrovně logování
n) Postupy pro vytvoření prostředí pro umožnění vývoje a testování externích informačních systémů napojených na DMS (převážně přes WS), včetně možnosti testování změn v DMS a přípravy na ně externími odběrateli – Dodavatel očekává vytvoření prostředí pro účely vývoje systémů třetích stran. Může jít o plnohodnotné testovací prostředí, které bude Dodavatel udržovat, nebo o zajištění rozhraní pro testování se simulovanými daty (mock služby). Způsob vytvoření prostředí a jeho dokumentace bude předmětem dohody s dodavatelem.

Dodavatel bude dodávat nové verze systému v plánovaných termínech. V případě nutnosti Dodavatel připraví mimořádnou dodávku (Patch), která bude nasaditelná mimo takto plánované termíny. Metodologie výroby Dodavatele je na takový postup připravená. Kód je ukládán ve větvích verzovacího nástroje Git. Vývoj nové verze vždy probíhá v nové větvi. Stav u zákazníka reflektuje základní větev, ve které je možné provádět opravy na stavu prostředí, které je u zákazníka. Z tohoto prostředí Dodavatel vygeneruje tzv. hotfix, který je ještě před nasazením na prostředí zákazníka testován.

Všechny verze včetně hotfixů Dodavatel zaznamenává a eviduje požadavky a vady, které tyto verze obsahují a opravují. Všechny změny provedené ve verzi Dodavatel dokládá v protokolu přiloženému k verzi.

Práva a povinnosti manažera a architekta kybernetické bezpečnosti VIS

1 Úvod

Práva a povinnosti manažera i architekta kybernetické bezpečnosti uvedené v tomto dokumentu se týkají VIS DMS.

2 Práva a povinnosti manažera kybernetické bezpečnosti VIS

Manažer kybernetické bezpečnosti VIS odpovídá za systém řízení bezpečnosti informací pro daný VIS a odpovídá se manažeru kybernetické bezpečnosti Zadavatele.

2.1 Povinnosti manažera kybernetické bezpečnosti VIS

- znalost ZoKB a jeho prováděcích vyhlášek,
- neprodleně hlásit manažerovi kybernetické bezpečnosti Zadavatele kybernetické bezpečnostní incidenty VIS a vést jejich evidenci,
- připravovat pro manažera kybernetické bezpečnosti Zadavatele podklady pro NÚKIB,
- za VIS připravovat pro manažera kybernetické bezpečnosti Zadavatele podklady pro jednání Výboru pro řízení kybernetické bezpečnosti,
- odpovídat za zajištění odstranění nedostatků zjištěných při kontrolách NÚKIB,
- zajišťovat provedení reaktivních opatření,
- poskytovat součinnost auditorovi kybernetické bezpečnosti a auditorům KÚ/ZÚ/ČÚZK při provádění auditů a kontrol,
- vyhodnocovat a klasifikovat kybernetický bezpečnostní incident,
- klasifikovat, prošetřovat a určovat příčiny kybernetického bezpečnostního incidentu, vyhodnocovat účinnost preventivních a reaktivních opatření aplikovaných proti kybernetickému bezpečnostnímu incidentu,
- dokumentovat zvládání kybernetických bezpečnostních incidentů,
- navrhovat úpravy bezpečnostní dokumentace na základě zjištění z auditů kybernetické bezpečnosti, výsledků vyhodnocení účinnosti systému řízení bezpečnosti informací a v souvislosti s prováděnými nebo plánovanými změnami ve VIS,
- zajišťovat provedení analýzy rizik a hodnocení aktiv,
- na základě výstupů analýzy rizik zpracovávat a vytvořit dokument *„Plán zvládání rizik“*,
- provádět aktualizaci dokumentu *„Zpráva o hodnocení aktiv a rizik“*, *„Plán zvládání rizik“*, a to nejméně jednou za 3 roky, nebo v souvislosti s prováděnými nebo plánovanými změnami významně ovlivňujícími bezpečnost informací,
- zpracovávat ve spolupráci s architektem kybernetické bezpečnosti VIS a garantem aktiv VIS dokument *„Prohlášení o aplikovatelnosti“*,
- připravovat podklady do dokumentu *„Zpráva z přezkoumání systému řízení bezpečnosti informací“* a předkládat je manažerovi kybernetické bezpečnosti Zadavatele,
- garantovat implementaci schválených bezpečnostních opatření,
- zohledňovat, do měsíce od informování manažerem kybernetické bezpečnosti Zadavatele, reaktivní a ochranná opatření vydaná NBÚ (nyní NÚKIB) v dokumentu *„Zpráva o hodnocení aktiv a rizik“* a v případě, že hodnocení rizik aktualizované o nové zranitelnosti spojené s realizací reaktivního nebo ochranného opatření překročí stanovená kritéria pro přijatelnost rizik, doplní dokument *„Plán zvládání rizik“*. Splnění oznámí manažerovi kybernetické bezpečnosti,
- stanovovat provozní pravidla a postupy, k zajištění bezpečného provozu VIS, v dokumentu *„Politika řízení provozu a komunikací“*,
- odpovídat za kontrolu přidělování jednoznačného identifikátoru uživatelům VIS,
- stanovovat bezpečnostní požadavky na změny VIS spojené s jeho akvizicí, vývojem a údržbou a uplatňovat jejich zahrnutí do projektu, jehož součástí je akvizice, vývoj a údržba daného VIS,
- zpracovávat na základě bezpečnostních potřeb a výsledků hodnocení rizik dokument *„Prohlášení o aplikovatelnosti“*,

- zajistit vyhodnocení oznámených kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů detekovaných technickými nástroji, provádět jejich vyhodnocení a přijímat opatření k minimalizaci dopadů v důsledku jejich působení,
- komunikovat s ostatními bezpečnostními rolemi daného VIS za účelem zajištění kybernetické bezpečnosti,

2.2 Práva manažera kybernetické bezpečnosti VIS
- řídit a spolupracovat s architektem kybernetické bezpečnosti VIS, garantem aktiv VIS a administrátory technických aktiv pro zajištění splnění požadavků ZoKB a VoKB, k tomu vyžadovat součinnost a plnění úkolů,
- vyžadovat spolupráci a konzultaci s manažerem kybernetické bezpečnosti Zadavatele,
- v případech, kdy nelze pravidla, postupy a opatření stanovená v bezpečnostních dokumentech nebo uvedená v ZoKB a VoKB naplnit nebo VIS neumožňuje jejich aplikaci, předkládat opodstatněnou žádost o výjimku, prostřednictvím manažera kybernetické bezpečnosti Zadavatele, ke schválení Výboru pro řízení kybernetické bezpečnosti.

3 Práva a povinnosti architekta kybernetické bezpečnosti VIS

Architekt kybernetické bezpečnosti VIS zajišťuje návrh a implementaci bezpečnostních opatření. Odpovídá za návrh bezpečné architektury VIS a jeho následnou implementaci.

3.1 Povinnosti architekta kybernetické bezpečnosti VIS:
- znalost ZoKB a jeho prováděcích vyhlášek,
- implementovat rozhodnutí NÚKIB o reaktivním opatření, ochranném opatření nebo varování,
- posuzovat zajištění bezpečnosti prvků, které tvoří podpůrná aktiva ve vazbě na primární aktiva,
- určovat klíčové podmínky, principy a modely architektury VIS, posuzovat a vybírat technologie a stanovovat koncepci bezpečnostního rozvoje VIS,
- připomínkovat bezpečnostní architekturu informačních a komunikačních systémů včetně podpůrných technických aktiv,
- definovat požadavky na nástroje pro zajištění technických opatření kybernetické bezpečnosti,
- odpovídat za popis zajištění fyzické bezpečnosti VIS v dokumentu *„Politika fyzické bezpečnosti“*,
- odpovídat za obsah a aktuálnost dokumentu *„Politika řízení provozu a komunikací“* VIS,
- dohlížet na implementaci bezpečnostních opatření,
- navrhovat opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu,
- poskytovat součinnost dalším bezpečnostním rolím,
- na žádost garanta aktiv VIS analyzovat úrovně architektury kybernetické bezpečnosti, definovat pro ni metriky a identifikovat existující rizika a navrhovat strategii pro zmírnění rizik,
- vytvářet a udržovat model architektury kybernetické bezpečnosti (procesní model, aplikační architekturu, technologie atd.),
- manažerovi kybernetické bezpečnosti VIS předkládat návrhy změn bezpečnostních dokumentů,
- na Výbor pro řízení kybernetické bezpečnosti navrhovat změny architektury kybernetické bezpečnosti,
- vytvářet a pravidelně aktualizovat dokument *„Strategie řízení kontinuity činností“* pro VIS,
- ve spolupráci s manažerem kybernetické bezpečnosti VIS a garantem aktiv VIS zajistit minimálně 1x ročně aktualizaci a otestování plánů obnovy VIS,
- navrhovat opatření pro zvýšení odolnosti VIS vůči kybernetickým incidentům s využitím technických nástrojů pro zajišťování stanovené úrovně dostupnosti,
- stanovovat a aktualizovat postupy pro provedení opatření vydaných NÚKIB, se zohledněním výsledků hodnocení rizik, provedených opatření, stavu dotčených bezpečnostních opatření a vyhodnocovat případné negativní dopady na provoz a bezpečnost VIS,
- odpovídat za aktuálnost dokumentu *„Politika bezpečnosti komunikační sítě“*, v kterém dokumentuje též užití nástroje zajišťujícího ochranu integrity vnitřní komunikační sítě,
- odpovídat za to, že Dodavatel provede bezpečnostní testy zranitelnosti aplikací, minimálně těch, které jsou přístupné z vnější sítě, a to před jejich uvedením do provozu a po každé zásadní konfigurační změně, změně topologie infrastruktury, použitého operačního systému nebo

aplikačního softwaru anebo změně bezpečnostních mechanismů. O provedení bezpečnostní testů předává manažerovi kybernetické bezpečnosti VIS *„Zprávu o výsledku provedení bezpečnostních testů“* s návrhy opatření,

- komunikovat s ostatními bezpečnostními rolemi VIS pro zajištění kybernetické bezpečnosti.

3.2 Práva architekta kybernetické bezpečnosti VIS:

- vyžadovat součinnost garanta aktiv VIS a manažera kybernetické bezpečnosti VIS.

Seznam bezpečnostní dokumentace pro DMS

Plný název resortní bezpečnostní politiky	**Zkrácený název**
Politika systému řízení bezpečnosti informací	BP-SRBI
- Pravidla a postupy pro řízení bezpečnostní dokumentace	BD-PP-RBD
- Seznámení s bezpečnostní dokumentací	
- Pravidla a postupy pro provádění auditů a kontrol kybernetické bezpečnosti	BD-PP-PAK
Politika řízení aktiv	BD-BP-RA
Politika organizační bezpečnosti	BD-BP-OB
Politika řízení dodavatelů	BD-BP-RD
Politika bezpečnosti lidských zdrojů	BD-BP-LZ
Politika řízení provozu a komunikací	BD-BP-RPK
Politika řízení přístupu	BD-BP-ŘP
Politika bezpečného chování uživatelů	BD-BP-BCHU
Politika zálohování a obnovy a dlouhodobého ukládání	BD-BP-ZODU
Politika bezpečného předávání a výměny informací	BD-BP-BPVI
Politika řízení technických zranitelností	BD-BP-RTZ
Politika bezpečného používání mobilních zařízení	BD-BP-BPMZ
Politika akvizice, vývoje a údržby	BD-BP-AVU
Politika ochrany osobních údajů	BD-BP-OOU
Politika fyzické bezpečnosti	BD-BP-FB
Politika bezpečnosti komunikační sítě	BD-BP-BKS
Politika ochrany před škodlivým kódem	BD-BP-OSK
Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí	BD-BP-NPNDKBU
Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí	BD-BP-VUNSVKBU
Politika bezpečného používání kryptografické ochrany	BD-BP-BPKO
Politika řízení změn	BD-BP-RZ
Politika zvládání kybernetických bezpečnostních incidentů	BD-BP-ZKBI
Politika řízení kontinuity činností	BD-BP-RKC
Politika havarijního plánování ČÚZK	BD-BP-HP

Plný název resortního bezpečnostního dokumentu	Zkrácený název
Metodika pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik	BD-ME-IHAHR
Plán rozvoje bezpečnostního povědomí	BD-PL-RBP
Evidence změn	BD-PP-EZ
Přehled obecně závazných právních předpisů vnitřních předpisů a jiných předpisů a smluvních závazků	BD-P-OZP

Plný název bezpečnostního dokumentu DMS	Zkrácený název
DMS Zpráva o hodnocení aktiv a rizik	BD001
DMS Hodnocení rizik	BD001A
DMS Prohlášení o aplikovatelnosti	BD002
DMS Plán zvládání rizik	BD003
DMS Strategie řízení kontinuity činností	BD004
DMS – Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků vztahujících se k DMS	BD005
DMS – Metodika bezpečnostního testování DMS	BD011

Zajištění bezpečnostních testů

1 Úvod

Tento dokument stanovuje pravidla a postupy pro provádění bezpečnostních testů v prostředí Zadavatele k zajištění bezpečnostního testování DMS (dále též „bezpečnostní testování“ nebo „bezpečnostní testy“).
Interní testování Dodavatele v oblasti bezpečnosti prováděné na technologické infrastruktuře Dodavatele není obsahem tohoto dokumentu.

2 Členění zranitelností podle závažnosti

2.1 CRITICAL

Kritická, vyžaduje zpravidla okamžitý zásah nebo odstavení systému.

2.2 IMPORTANT

Důležitá, může být zdrojem budoucích potíží, je nezbytná náprava dle možností co nejdříve.

2.3 MEDIUM

Střední stupeň závažnosti, zvyšuje pravděpodobnost úspěšného útoku, zpravidla vyžaduje splnění určitých podmínek.

2.4 LOW

Nízký stupeň závažnosti, pouze mírně zvyšuje pravděpodobnost úspěšného útoku, vyžaduje splnění určitých podmínek.

2.5 INFORMATION

Informativní, nejedná se ve skutečnosti o zranitelnost, ale o informaci.

3 Pravidla a způsob provádění bezpečnostních testů

Bezpečnostní testování bude prováděno v testovacím prostředí Zadavatele a v předem stanoveném a Zadavatelem odsouhlaseném rozsahu.
Výjimky z rozsahu bezpečnostních testů jsou možné pouze po předchozím odsouhlasení Zadavatele.

3.1 Kritéria pro stanovení rozsahu bezpečnostního testování

Bezpečnostní testování může být vyvoláno následujícími faktory:

3.1.1 Příprava dodávky DMS

Dodavatel při navrhování rozsahu bezpečnostního testu posuzuje:

- zda změna DMS zasahuje přímo do bezpečnostních vlastností DMS (změna je s přímým bezpečnostním dopadem, např. zavedení nové webové služby, změna technologie), nebo zda změna má nebo může mít nepřímý bezpečnostní dopad nebo zda může zasáhnout do bezpečnostních opatření DMS (např. doplněný nebo změněný modul bez přímé vazby na bezpečnostní opatření),
- rozsah změn DMS.

Závazný minimální rozsah bezpečnostních testů, v závislosti na charakteru změny vyjádřené číslem verze dodávky, je uveden v následující tabulce.

Označení změny	Označení verze	Rozsah dodavatelem prováděných testů
Významná změna	X.Y (např. 3.0, 3.1, ..)	Bude vždy provedena kompletní sada bezpečnostních testů dle kapitoly Bezpečnostní testy webových aplikací a služeb tohoto dokumentu.
Změna	X.Y.Z (např. 3.0.1, 3.1.2, …)	Bude provedena kompletní sada bezpečnostních testů pouze v případě, že bude implementována alespoň jedna změna DMS s možným přímým nebo nepřímým bezpečnostním dopadem.

Patch/Hotfix	X.Y.Z.xx (např. 3.0.1.03)	Dodavatelem budou provedeny bezpečnostní testy vybraných a navržených testovacích scénářů pro příslušnou změnu s možným bezpečnostním dopadem, případně i další bezpečnostní testy navržené Zadavatelem nad rámec návrhu Dodavatele.
Změna bezpečnostního mechanismu		Budou provedeny bezpečnostní testy Dodavatelem vybraných a navržených bezpečnostních testovacích scénářů pro příslušnou změnu na základě povahy této změny.
Nová hrozba		Budou provedeny bezpečnostní testy vybraných a případně nově navržených bezpečnostních testovacích scénářů pro příslušnou hrozbu na základě povahy této hrozby. Návrh dá vždy Dodavatel, Zadavatel ale může navrhnout vlastní bezpečnostní scénář.

Bezpečnostní testy začleňuje Dodavatel do harmonogramu dané dodávky. Pokud není v období 12 měsíců plánována / dodána dodávka DMS typu X.Y, začlení Dodavatel provedení kompletní sady bezpečnostních testů do vhodné dodávky DMS typu X.Y.Z tak, aby odstup od minulého provedení kompletní sady bezpečnostních testů nebyl větší než 12 měsíců, případně lze po dohodě se Zadavatelem provést na v té době vhodném testovacím prostředí Zadavatele kompletní sadu bezpečnostních testů bez vazby na konkrétní dodávku DMS.

3.1.2 Zjištění výskytu relevantní zranitelnosti v průběhu kybernetického bezpečnostního incidentu

V takovém případě je bezpečnostní testování prováděno v rozsahu nezbytném pro ověření, zda kybernetický bezpečnostní incident nebyl způsoben zranitelností. Provedení bezpečnostních testů navrhuje Dodavatel na základě zjištěných informací; součástí návrhu je i vhodné začlenění do harmonogramů aktuálních/plánovaných dodávek.

3.2 Informace zjištěné při činnostech prováděných Manažerem nebo Architektem kybernetické bezpečnosti VIS nebo Specialistou kybernetické bezpečnosti

Zdrojem těchto informací může být například sledování informačního servisu NÚKIB nebo security bulletinů; v takovém případě je bezpečnostní testování prováděno, pokud obsahuje komponentu, která může být na zranitelnost náchylná; účelem tohoto bezpečnostního testu je zjištění, zda DMS danou zranitelnost obsahuje. Provedení bezpečnostní testů navrhuje Dodavatel na základě zjištěných informací; součástí návrhu je i vhodné začlenění do harmonogramů aktuálních/plánovaných dodávek.

3.3 Pravidelné bezpečnostní testy na produkčním prostředí

Dodavatel provádí na produkčním prostředí Zadavatele pravidelně minimálně 1 x za 12 měsíců sadu základních bezpečnostních testů v rozsahu Přílohy č. 1.

Pravidla provádění bezpečnostních testů

Bezpečnostní testy musí být opakovatelné, aby se výsledky jednotlivých testů daly porovnat a vyhodnotit stav a vývoj bezpečnosti aplikace.

Testy musí být prováděny jak:

- neinvestigativním způsobem, tj. prověření správné implementace bezpečnostních mechanismů v aplikacích, shody s návrhem bezpečnostní architektury a shody vůči relevantním systémovým bezpečnostním politikám,
- tak i investigativním způsobem při realizaci změn webových aplikací, které mohou mít dopad na zajištění důvěrnosti, dostupnosti a integrity aktiv.

Bezpečnostní testování provádí Dodavatel, na základě Dodavatelem předem zpracovaných testovacích scénářů.

3.4 Způsob provádění bezpečnostních testů

Interní testování Dodavatele

Na základě schváleného harmonogramu implementace dané změny DMS provede Dodavatel interní testování v testovacím prostředí Dodavatele s instalovanou změnou (tj. před schválením instalace změny

do produkčního prostředí ČÚZK). V případě zjištění bezpečnostní chyby nebo zranitelnosti již v testovacím prostředí Dodavatele, Dodavatel zajistí odstranění chyby a opakování bezpečnostních interních testů.

Testování v prostředí Zadavatele

Na základě změny DMS Dodavatel předá garantovi aktiv DMS a manažerovi kybernetické bezpečnosti resortu před zahájením celkového testování informaci o seznamu změn DMS, včetně uvedení, jak danou změnu vyhodnotil, tj. zda tato změna má nebo nemá bezpečnostní dopad a jaký rozsah bezpečnostních testů bude dle tohoto dokumentu minimálně proveden, včetně harmonogramu celkového testování s vyznačením termínů provádění bezpečnostních testů, tj. dodání dokumentu „Plán bezpečnostního testování pro dodávku X“, který musí vždy obsahovat všechny změny DMS, které dodávka zahrnuje, vliv změn na bezpečnost a uvedení, zda změny budou testovány z hlediska bezpečnosti.

Dokument „Plán bezpečnostního testování pro dodávku X“ podléhá schválení ředitele odboru informatiky ČÚZK.

Na základě schváleného dokumentu „Plán bezpečnostního testování pro dodávku X“ provede Dodavatel testování po instalaci nové změny do provozního prostředí Zadavatele, kde se provádějí bezpečnostní testy webových aplikací a webových služeb a penetrační testy uvedené v bodu 4 tohoto dokumentu.

Pro účely testování poskytne Zadavatel Dodavateli:

- testovací účet s přístupem do DMS a jejích webových aplikací a služeb s právy běžného interního uživatele,
- vzdálený přístup do interní sítě Zadavatele, nebo fyzický přístup na pracoviště Zadavatele pokud to bude pro testování potřebné;
- možnost připojení koncového zařízení Dodavatele (testovacího notebooku nebo serveru) do testovacího prostředí Zadavatele.

Dodavatel je při provádění bezpečnostních testů povinen:

- bezpečnostní testy provádět dle schváleného dokumentu „Plán bezpečnostního testování pro dodávku X“;
- neprovádět nevratné zásahy do systému (v případě úspěšného průniku);
- nepoužívat techniky „sociálního inženýrství“ (telefonáty nebo maily pod předstíranou identitou apod.);
- v případě zjištění závažné skutečnosti v průběhu testování (odstavení některé služby, zjištění závažné slabiny apod.) okamžitě informovat garanta aktiv DMS.

Výsledky bezpečnostních testů zpracuje Dodavatel do Zprávy o výsledcích bezpečnostních testů a předloží ji i s návrhy opatření a uvedením způsobu, jakým byly zjištěné kritické zranitelnosti vyřešeny Zadavateli. V případě, že zpráva obsahuje zjištěné zranitelnosti, Dodavatel zajistí svolání schůzky Dodavatele se Zadavatelem, kde prezentuje své zjištění a blíže informuje o návrhu/návrzích řešení. Na schůzce Zadavatel rozhodne o způsobu odstranění zranitelností nebo jejich eliminaci a dalším postupu. Závěry ze schůzky Dodavatel zaznamená do zápisu ze schůzky, který podepisuje zástupce Dodavatele a garant aktiv DMS.

Bez akceptace nemůže být změna instalována do provozního prostředí Zadavatele. Nalezené kritické zranitelnosti v oblasti bezpečnosti přitom musí být vždy Dodavatelem napraveny a opakovaně ověřeny bezpečnostním testem.

Ochrana dat v průběhu testování

Dodavatel se v průběhu realizace bezpečnostních testů řídí standardními pravidly pro zajištění důvěrnosti používaných informací, zejména pak:

- tam, kde je to možné, používá anonymizované informace,
- v případech, kdy použití anonymizovaných informací není možné (např. v rámci testování v produkčním prostředí), je povinen zajistit opatření, která znemožní jejich nekontrolovaný únik.

4 Bezpečnostní testy webových aplikací a služeb

V rámci bezpečnostních testů jsou testována rozhraní DMS, k nimž přistupují uživatelé, jak interní z vnitřní sítě resortu, tak externí, kteří mají přístup zajištěn pomocí dálkového přístupu z vnější sítě.

Bezpečnostní testy musí obsahovat vždy otestování:

a) syntaxe všech uživatelských postupů
b) odolnosti proti známým typům útoků (XSS, CSRF, Session Steal, ClickJacking apod.),
c) zákazu používání tzv. skrytých polí pro důvěrná (citlivá) data,
d) zákazu používání přídavných identifikací uživatelských „session“ a obdobných autentizačních prostředků zakomponovaných v URL,
e) zákazu uvádění názvů souborů a adresářových cest v chybových hlášeních,

f) možností uživatelova odhlášení a automatického odhlášení po definované době jeho nečinnosti,
g) omezení pro používání Cookies na Cookies s časově omezenou platností, které jsou posílány zpět pouze stejnému serveru,
h) Java applety a případné jiné komponenty musí být podepsány důvěryhodnou certifikační autoritou,
i) komunikace aplikace s datovými zdroji v interní síti musí být autentizovaná,
j) možnost napadení DoS útokem,

případně další zranitelnosti definované tímto dokumentem (specifické testy).

4.1 Penetrační testy

Při penetračním testu Dodavatel minimálně simuluje útok neoprávněné osoby z vnější sítě.
Penetrační testy se provádějí, z hlediska efektivity a správnosti, s částečnou znalostí testovaného cíle, tzv. „gray box".
Cílem budou prověřovány ve dvou úrovních a to:

- identifikace a prověření známých zranitelností na úrovni standardních webových služeb serveru;
- a identifikace a prověření známých zranitelností na úrovni architektury vlastní webové aplikace.

Penetrační testy musí vždy ověřit, zda webová aplikace, resp. webová služba, neobsahuje žádnou ze všech známých zranitelností uvedených v Příloze č. 1, bodu 1 tohoto dokumentu, spadajících pod OWASP TOP 10 – 2017 (**https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf**), nebo aktuální.
Za tímto účelem jsou realizovány odpovídající testovací scénáře uvedené v Příloze č. 1 tohoto dokumentu.
Zadavatel připouští realizaci bezpečnostních testů níže uvedenými způsoby, přičemž jejich použití k ověření oblastí testování v Příloze č. 1 ponechává na Dodavateli.

4.1.1 Automatizované testy a automatizované testy s manuálním podílem

Pro automatizované testy a automatizované testy s manuálním podílem bude použit některý ze SW nástrojů. Druh aktuálně použitého SW nástroje uvede Dodavatel v dokumentu PBT.

4.1.2 Manuální testování

Manuální testování provede Dodavatel v těch případech, kdy není možné využít automatizované testy nebo by použití automatizovaných testů nebylo dostatečně efektivní.

1.1 Specifické testy

Metodika OWASP obsahuje standardizované testy, tj. nezahrnuje všechny testovací scénáře zranitelností, které se mohou při vývoji informačního systému vyskytnout. Vzhledem k tomu budou dále pro zajištění bezpečného fungování DMS prováděny též i další specifické testy.
Specifické testy budou vycházet a zohledňovat možná specifika kódu, zjištění ze sledování informačního servisu NÚKIB apod., zranitelnosti zjištěné při provozu DMS, které se vyskytly jako bezpečnostní události nebo incidenty u nichž je nutné zajistit přijetí bezpečnostní opatření k zajištění jejich neopakovatelnosti nebo eliminaci a které vznikly v době před odpovídající aktualizací metodiky OWASP.
Seznam testovacích scénářů pro specifické testy je uveden v Příloze č. 1 tohoto dokumentu.

5 Předmět bezpečnostních testů DMS

Předmětem bezpečnostních testů DMS je:

- **https://dms-p.cent.priv/urm/**

Dodavatel je vždy povinen zahrnout do testování další nové externí a interní části DMS a dle toho aktualizovat tento dokument.

6 Testovací scénáře

Testovací scénáře musí zahrnovat následující údaje:

- název testovacího scénáře,
- ID testovacího scénáře,
- Tester – jméno
- verze systému,
- počet provedení scénáře,

- účel testu – popis, co je testem ověřováno,
- výchozí stav systému a vstupní podmínky,
- kroky testu – popis testovacích kroků a dat používaných pro testování,
- očekávané výsledky – kritéria úspěšnosti testu přiřazené ke každému z testovacích kroků.

7 Zpráva o výsledcích bezpečnostních testů

O provedení bezpečnostních testů pořizuje Dodavatel Zprávu o výsledku bezpečnostních testů.
Zpráva musí vždy obsahovat minimálně:

- Datum a čas provedení bezpečnostního testu
- Na jakém prostředí bylo testováno
- Změny aplikace, které jsou dodávány
- Seznam změn, které podléhají/nepodléhají bezpečnostním testům
- ID testovacího scénáře
- Jméno testera, který testování prováděl
- Manažerský souhrn s důležitými závěry bez technických detailů
- Technickou zprávu shrnující zjištění s technickými detaily a protokoly z testování
- Soupis zjištění
- Je-li součástí zprávy report generovaný nějakým SW nástrojem, je nutné specifikovat název a verzi nástroje, případně verzi pluginů. Zjištění musí být v celé zprávě jednotně klasifikována, přestože jsou použity různé SW nástroje, které mohou mít vlastní klasifikace

Sumarizaci zjištěných zranitelností/závad/slabin, včetně jejich závažnosti podle CVSS. Zprávu o výsledku bezpečnostních testů předá Dodavatel garantovi aktiv DMS nejpozději do 5-ti pracovních dnů od ukončení bezpečnostních testů.
Nalezené kritické zranitelnosti (CVSS>7) oznamuje dodavatel garantovi aktiv DMS neodkladně po nalezení kritické zranitelnosti.

8 Přechodná ustanovení

Pro provádění testů se vychází ze standardu OWASP TOP10:2017 a metodologie testování podle OWASP v 4.0 (OWASP Testing Guide v4). Dodavatel se zavazuje, že v případě uvolnění nové verze OWASP Top10 nebo OWASP Testing Guide bude tento dokument do měsíce od vydání nové verze OWASP aktualizovat v souladu s novou verzí a upravit i odpovídající testovací scénáře a používat odpovídající postupy.

9 Příloha č. 1 - Seznamy testovaných zranitelností, testovacích scénářů a specifických zranitelností

Seznam zranitelností podle OWASP Top 10 – 2017
01: Injection
Zranitelnost typu injektáže (SQL, LDAP, XPath, NoSQL dotazů; příkazů operačního systému, XML parsování, SMTP hlaviček, programových argumentů, atd.) je velmi běžnou chybou webových aplikací, které nastává, pokud jsou přes neošetřený vstup uživatelem poskytnutá nedůvěryhodná data poslána do překladače jako část příkazu nebo dotazu. Např. u „SQL injection“ jde o vykonání vlastního, pozměněného SQL dotazu za účelem neoprávněného přístupu k informacím, jejich změně nebo i ovládnutí daného zařízení. Zranitelnosti typu injektáže lze snadno zjistit při revizi kódu, ale těžší je zjišťovat jejich přítomnost pomocí testů vzhledem k velké variabilitě manipulace parametrů http dotazů.

A02: Broken Authentication
Vývojáři často vytváří autentizační mechanismy a řízení relací, ale jejich správné vytvoření není jednoduché. Jako výsledek těchto snah bývají často zranitelnosti v oblastech odhlášení, správy hesel, dlouhé časové limity pro relace, aktualizace účtů atd. Útočníci mohou kompromitovat hesla, klíče nebo autentizační identifikátory k předstírání jiných uživatelských identit. Nalezení těchto zranitelností může být občas těžké, protože každá takováto implementace bývá jedinečná.

A03: Sensitive Data Exposure
Nejběžnější chybou je nešifrování citlivých dat. Pokud se používá šifrování, jde o generování slabých klíčů, použití slabých šifrovacích algoritmů nebo slabé hashovací techniky pro hesla. Zranitelnosti v prohlížeči jsou velmi časté a snadno odhalitelné, ale těžko zneužitelné ve velkém měřítku.

A04: XML External Entities (XXE)

Ve výchozím nastavení mnoho starších procesorů XML umožňuje specifikaci externí entity, URI, která je dereferencována a vyhodnocena během zpracování XML. Nástroje SAST mohou tento problém zjistit kontrolou závislostí a konfigurace. Nástroje DAST vyžadují další ruční kroky k odhalení a zneužití tohoto problému. Jde o novou zranitelnost, zatím nebyla testována.

A05: Broken Access Control
Aplikace často používají skutečný název nebo klíč objektu při generování webových stránek. Aplikace ne vždy ověřuje, zda je uživatel oprávněn přistupovat k cílovému objektu. Útočník tak může neoprávněně manipulovat s těmito odkazy a přistupovat k jiným objektům (bez autorizace). Testeři můžou snadno manipulovat hodnoty parametrů k detekci takovýchto zranitelností. Analýza kódu rychle ukáže, zda povolení je řádně ověřeno.

A06: Security Misconfiguration
Bezpečnostně chybná konfigurace může nastat na jakékoliv úrovni infomačního systému ať už to je webový server, aplikační server, databáze, framework, atd. Vývojáři a systéméví administrátoři musí úzce spolupracovat, aby zajistili, že konfigurace všech částí infomačního systému je v pořádku. Automatizované scannery jsou vhodné pro detekci chybějících patchů, použití defaultních účtů, nepotřebných služeb, apod..

A07: Cross Site Scripting (XSS)
XSS je nejrozšířenější zranitelnost webových aplikací. XSS zranitelnost nastává, pokud aplikace zahrne uživatelem poskytnutá data do webové stránky a pošle ji do prohlížeče, aniž by tato data řádně validoval nebo byly escapovány. To umožní ve webovém prohlížeči oběti spustit útočníkův skript, který může např. neoprávněně převzít uživatelskou relaci, změnit obsah stránek, instalovat škodlivé programy apod. Detekce většiny XSS zranitelností je poměrně snadná jak testováním, tak i revizí kódu nebo konfigurací webového serveru.

A08: Insecure Deserialization
Tato zranitelnost je zahrnuta do Top 10 na základě průzkumu v oboru, nikoli na kvantifikovatelných údajích o výskytu. Některé nástroje mohou objevit chyby v deserializaci, ale pro potvrzení problému je často potřeba pomoc člověka. Očekává se, že údaje o prevalenci v případě nedostatků způsobených deserializací se zvýší, protože nástroj je stále vyvíjen, aby pomohl identifikovat a řešit problém. Dopad deserializačních zranitelností nemůže být podceňován. Tyto zranitelnosti mohou vést k útokům typu vzdálené spuštění kódu, což je jeden z nejzávažnějších možných útoků.

A09: Using Components with Known Vulnerabilities
Prakticky každá aplikace má problémy s použitím komponent (knihovny, frameworky a další softwarové moduly) obsahujících známé zranitelnosti, protože většina vývojářů se nesoustředí na zajištění aktualizací komponenty/knihoven. V mnoha případech vývojáři ani neznají, jaké všechny komponenty se používají, natož jejich verze. Závislosti komponent situaci ještě zhoršují. Detekce se provádí zpravidla lokálně v rámci zdrojového kódu, ale částečně ji lze provést i pomocí penetračního testu.

A10: Insufficient Logging & Monitoring
Tato zranitelnost je zahrnuta do Top 10 na základě průzkumu v oboru, nikoli na kvantifikovatelných údajích o výskytu. Jedna z možných strategií pro zjištění, zda je správně nastaven monitoring a logování, je prověřit protokoly po penetračním testování. Činnosti testerů by měly být dostatečně zaznamenány, aby bylo možné zjistit, jaké škody by mohly být způsobeny. Nejúspěšnější útoky začínají zkoumáním zranitelnosti. Povolení pokračování takových zkoumání může zvýšit pravděpodobnost úspěšného útoku téměř na 100%.

Seznam specifických zranitelností
Aktuálně bez specifických zranitelností testovaných specifickými testy.
Testovací scénáře OWASP (dle OWASP Testing Guide v4.0)

Information Gathering (Sběr informací)	
OTG-IG-001 - 4.2.1 Conduct search engine discovery/reconnaissance for information leakage	Provést sběr informací o cíli s využitím vyhledávače Google. Provést sběr informací o cíli s využitím robots.txt.
OTG-IG-002 - 4.2.2 Fingerprint Web Server	Najít verzi a typ běžícího webového serveru, aby se zjistili známá zranitelná místa a příslušné zneužití, které je třeba použít při testování

OTG-IG-003 - 4.2.3 Review Webserver Information Leakage Metafiles for	Analyzovat robots.txt Webmaster Tools. použitím Google
OTG-IG-004 - 4.2.4 Enumerate Applications on Webserver	Identifikovat aplikace, které existují v daném rozsahu. Black box pentest
OTG-IG-005 - 4.2.5 Review Webpage Comments and Metadata for Information Leakage	Zjistit jaká webová aplikace běží na webovém serveru.
OTG-IG-006 - 4.2.6 Identify application entry points	Analyzovat, jak jsou vytvářeny požadavky a typické odpovědi z aplikace
OTG-IG-007 - 4.2.7 Map execution application paths through	Mapování cílové aplikace a pochopení hlavních pracovních postupů.
OTG-IG-008 - 4.2.8 Fingerprint Web Application Framework	Definovat typ použitého webového rámce tak, aby se upřesnila metodika testování zabezpečení.
OTG-IG-009 - 4.2.9 Fingerprint Web Application	Identifikace webové aplikace a verze, aby se zjistili známá zranitelná místa a příslušné zneužití, které je třeba použít při testování.
OTG-IG-010 - 4.2.10 Map Application Architecture	Analyzovat architekturu aplikace a mapovat vzájemné vazby mezi aplikací a dalšími programy.

Configuration and Deployment Management Testing (Testování managementu konfigurace a nasazení)	
OTG-CONFIG-001 - 4.3.1 TestNetwork/Infrastructure Configuration	Otestovat konfiguraci infrastruktury, podporuje aplikaci, identifikovat slabá v zabezpečení RUIAN. která místa
OTG-CONFIG-002 - 4.3.2 Test Application Platform Configuration	Přezkoumání a testování konfigurace. Testování přítomnosti defaultních nastavení, jako např. Directory traversal vulnerability, Use of sendmail.jsp atd.
OTG-CONFIG-003 - 4.3.3 Test File Extensions Handling for Sensitive Information	Určení způsobu, jakým webové servery zpracovávají požadavky odpovídající souborům s různými rozšířeními, mohou pomoci pochopit chování webového serveru v závislosti na druhu souborů, ke kterým je přístup.
OTG-CONFIG-004 - 4.3.4 Review Old, Backup and Unreferenced Files for Sensitive Information	Prověřit a vyhledat nereferenční nebo zapomenuté soubory, které lze použít k získání důležitých informací o infrastruktuře
OTG-CONFIG-005 - 4.3.5 Enumerate Infrastructure and Application Admin Interfaces	Rozhraní správce mohou být nastaveny v aplikaci nebo na aplikačním serveru, což umožňuje určitým uživatelům provádět privilegované činnosti na webu. Provést testy s cílem zjistit, zda a jak může tato privilegovaná funkce získat přístup neoprávněnému nebo standardnímu uživateli.
OTG-CONFIG-006 - 4.3.6 Test HTTP Methods	Zjistit povolené http metody a možnosti jejich zneužití včetně Cross Site Tracing (XST).
OTG-CONFIG-007 - 4.3.7 Test HTTP Strict Transport Security	Ověřit, zda web používá hlavičku HTTP, aby bylo zajištěno, že všechna data budou šifrována z webového prohlížeče na server.
OTG-CONFIG-008 - 4.3.8 Test RIA cross domain policy	Rich Internet Application (RIA) používá politiku Adobe crossdomain.xml pro řízení cross domain

	přístupů. Testovat konfiguraci soubory zásad popisujících omezení přístupu proti CSRF útokům.
OTG-CONFIG-009 - 4.3.9 Test File Permission	Testovat konfiguraci oprávnění souboru pro ochranu před zneužitím eskalace privilegií, injekci DLL nebo neoprávněným přístupem k souborům

Identity Management Testing (Testování managementu identit)	
OTG-IDENT-001 - 4.4.1 Test Role Definitions	Otestovat a pokusit se zachytit záhlaví paketů a jejich prohlížení. Využije se WebScarab nebo jiný libovolný webový proxy.
OTG-IDENT-002 - 4.4.2 Test User Registration Process	Ověřit, zda jsou požadavky na totožnost pro registraci uživatelů sladěny s požadavky definovaných politik a zabezpečení. Ověřit proces registrace, zda je validní.
OTG-IDENT-003 - 4.4.3 Test Account Provisioning Process	Prověřit existenci defaultních nebo snadno uhodnutelných uživatelských účtů. Ověřte, které účty mohou poskytovat další účty a jaký typ.
OTG- IDENT -004 - 4.4.4 Testing for Account Enumeration and Guessable User Account	Ověřit zda je možné získat uživatelská jména interakcí s autentizačním mechanismem aplikace. Provést útok hrubou silou na přihlašovací údaje.
OTG- IDENT - 005 - 4.4.5 Testing for Weak or unenforced username policy	Prověřit zda lze obejít autentizační mechanismus.

Autentification Testing (Testování Autentifikace)	
OTG-AUTH-001 - 4.5.1 Testing for Credentials Transported over an Encrypted Channel	Testovat, že uživatelská autentifikační data jsou přenášena přes šifrovaný kanál, aby se zabránilo zachycení útočníkem.
OTG- AUTH -002 - 4.5.2 Testing for default credentials	Provést test na přítomnost defaultních nebo známých uživatelských jmen a hesel pro zařízení v síti, která by vedla k úspěšné autentizaci
OTG- AUTH -003 - 4.5.3 Testing for Weak lock out mechanism	Prověřit aplikaci na možnou zranitelnost mechanismu blokování účtů odolnost vůči brute-force útokům. Vyhodnoťte odolnost mechanismu odblokování před neoprávněným odblokováním účtu
OTG-AUTH-004 - 4.5.4 Testing for Bypassing Authentication Schema	Zjistit zda lze obejít autentifikační opatření tím, že manipulujete s žádostmi a podváděním aplikace, že si uživatel již ověřil. Toho lze dosáhnout buď úpravou daného parametru adresy URL, manipulací s formulářem nebo paděláním relací.
OTG- AUTH -005 - 4.5.5 Testing for Vulnerable Remember Password	Hledejte hesla uložená v souboru cookie. Zkontrolujte soubory cookie uložené v aplikaci. Ověřte, zda pověření nejsou uložena v čistém textu, ale jsou šifrovaná. Prověřte mechanismus hashování: je-li to běžný, dobře známý algoritmus, zkontrolujte jeho sílu
OTG- AUTH -005 - 4.5.6 Testing for Browser cache weakness	Testovat zranitelnost prohlížeče na dříve zadané citlivé informace.
OTG- AUTH -005 - 4.5.7 Testing for Weak password policy	Testovat odolnost aplikace před brute-force útokům uhádnutí hesla pomocí dostupných slovníků hesel vyhodnocením požadavků na délku, složitost, opětovné použití a expiraci hesel.
OTG- AUTH -008 - 4.5.8 Testing for Weak security question/answer	Testovat na přítomnost lehce uhodnutelných otázek pro obnovu hesla.
OTG- AUTH -009 - 4.5.9 Testing for weak password change or reset functionalities	Určete odolnost aplikace proti možnosti změny účtu, která umožňuje někomu změnit heslo účtu. Určete odolnost funkce resetování hesel proti uhádnutí nebo obejití

OTG- AUTH-010 - 4.5.10 Testing for Weaker authentication in alternative channel	Provedení testů k identifikaci alternativních kanálů a, v závislosti na rozsahu testování, identifikovat zranitelnosti autentifikace.

Authorization Testing (Prověření autorizace)	
OTG-AUTHZ-001 - 4.6.1 Testing Directory traversal/file include	Testovat odolnost aplikace vůči Path Traversal útoku.
OTG- AUTHZ -002 - 4.6.2 Testing for bypassing authorization schema	Prověřit zda lze obejít autorizační mechanismus (např. přístup k funkcím/datům náležícím jiné uživatelské roli).
OTG- AUTHZ -003 - 4.6.3 Testing for Privilege Escalation	Prověřit aplikaci na zranitelnost typu eskalace privilegií.
OTG- AUTHZ -004 - 4.6.4 Testing for Insecure Direct Object References	Prověřit aplikaci na zranitelnost výskytu nesprávných odkazů na přímý objekt, když aplikace poskytuje přímý přístup k objektům založeným na uživatelském vstupu. V důsledku této zranitelnosti mohou útočníci obejít autorizaci a přístup k prostředkům přímo v systému, například databázové záznamy nebo soubory.

Session Management Testing (Správa relace)	
OWASP-SESS-001 - 4.7.1 Testing for Session Management Schema	Zkontrolovat cookie a jiné identifikátory relace zda jsou vytvořené bezpečným a nepředvídatelným způsobem.
OWASP- SESS -002 - 4.7.2 Testing for Cookies attributes	Prověřit správné nastavení cookie atributů.
OWASP- SESS -003 - 4.7.3 Testing for Session Fixation	Prověřit aplikaci na možnou zranitelnost session fixation (po úspěšné autentizaci se nezmění identifikátor relace).
OWASP- SESS -004 - 4.7.4 Testing for Exposed Session Variables	Zjistit zda jsou identifikátory relace dostatečně chráněné.
OWASP- SESS -005 - 4.7.5 Testing for CSRF	Testovat odolnost aplikace vůči CSRF útoku.
OWASP- SESS -006 - 4.7.6 Testing for logout functionality	Testovat možnost prvků uživatelského rozhraní, která umožňují uživateli ručně se odhlásit se. Ověřit nastavení ukončení relace po určitém čase bez aktivity (časový limit relace). Ověřit správné zneplatnění stavu relace na straně serveru.
OWASP- SESS -007 - 4.7.7 Test Session Timeout	Otestovat že aplikace automaticky odhlásí uživatele, když byl uživatel po určitou dobu nečinný
OWASP- SESS -008 - 4.7.8 Testing for Session puzzling	Testovat zabezpečení aplikace na přítomnost a používání stejné proměnné relace pro více než jeden účel.

Input Validation Testing (Testování validace dat)	
OTG-INPVAL-001 - 4.8.1 Testing for Reflected Cross Site Scripting	Prověřit existenci nepersistentních XSS (Cross Site Scripting) zranitelností.
OTG- INPVAL -002 - 4.8.2 Testing for Stored Cross Site Scripting	Prověřit existenci persistentních XSS (Cross Site Scripting) zranitelností.
OTG- INPVAL -003 - 4.8.3 Testing for DOM based Cross Site Scripting	Prověřit existenci DOM (document object model) XSS zranitelností.
OTG- INPVAL -004 - 4.8.4 Testing for HTTP Parametr polution	Prověřit existenci XSF (Cross Site Flashing) zranitelností.
OTG- INPVAL-005 - 4.8.5 SQL Injection	Prověřit existenci SQL Injection zranitelností.
OTG-DV-006 - 4.8.6 LDAP Injection	Prověřit existenci LDAP Injection zranitelností.

OTG-DV-007 - 4.8.7 ORM Injection	Prověřit existenci ORM Injection (Object Relational Mapping) zranitelností.
OTG-DV-008 - 4.8.8 XML Injection	Prověřit existenci XML Injection zranitelností.
OTG-DV-009 - 4.8.9 SSL Injection	Prověřit existenci SSI Injection (Server-Side Includes) zranitelností.
OTG-DV-010 - 4.8.10 XPath Injection	Prověřit existenci XPath Injection (XML Path Language) zranitelností.
OTG-DV-011 - 4.8.11 IMAP/SMTP Injection	Prověřit existenci IMAP/SMTP zranitelností.
OTG-DV-012 - 4.8.12 Testing for Code Injection	Prověřit existenci Code Injection zranitelností.
OTG-DV-012 - 4.8.12.1 Testing for Local File Inclusion	Prověřit existenci zranitelností (LFI) v podobě volání nějakého lokálního souboru skriptem.
OTG-DV-012 - 4.8.12.2 Testing for Remote File Inclusion	Prověřit existenci zranitelností (RFI) v podobě volání nějaké webové aplikace externím skriptem.
OTG-DV-013 - 4.8.13 Testing for Command Injection	Prověřit existenci zranitelností umožňující spuštění příkazů operačního systému.
OTG-DV-014 - 4.8.14 Testing for Buffer overflow	Prověřit existenci zranitelností umožňující přetečení zásobníku.
OTG-DV-015 - 4.8.15 Incubated vulnerability	Provést test vícenásobný zneužití zranitelností, kdy je např. nahrán škodlivý obsah aplikace uživatelům, kteří následně tento kód spustí.
OTG-DV-016 - 4.8.16 Testing for HTTP Splitting/Smuggling	Prověřit existenci zranitelností v http hlavičce.
OTG-DV-016 - 4.8.17 Testing for HTTP Incoming requests	Prověřit existenci zranitelností v http vstupním požadavku.

Testing for Error Handling (Testování zranitelností na dostupnost služeb)	
OTG-ERR-001 - 4.9.1 Analysis of Error Codes	Prověřit existenci Denial of Service (DoS) zranitelností na SQL zástupné znaky.
OTG-ERR-002 - 4.9.2 Analysis of Stack Traces	Zjistit zda lze pomocí špatně zadaných hesel uzamknout platný uživatelský účet.
OTG-DS-003 - 4.9.3 Testing for DoS Buffer Overflows	Zjistit zda lze pomocí přetečení zásobníku způsobit DoS.
OTG-DS-004 - 4.9.4 User Specified Object Allocation	Zkontrolovat, zda je možné vyčerpat zdroje serveru tím, že se alokuje velmi vysoký počet objektů.
OTG-DS-005 - 4.9.5 User Input as a Loop Counter	Zkontrolovat, zda je možné vnutit aplikaci smyčku prostřednictvím kódu segmentu, který potřebuje významnou část výpočetních zdrojů, aby se snížila celkovou výkonnost např. tím, že uživatel může přímo nebo nepřímo přiřadit hodnotu, která bude používána jako čítač ve smyčce.
OTG-DS-006 - 4.9.6 Writing User Provided Data to Disk	Zkontrolovat, zda je možné vyčerpat zdroje serveru tím, že se zaplní disk logy.
OTG-DS-007 - 4.9.7 Failure to Release Resources	Zkontrolovat, zda aplikace řádně uvolní zdroje (soubory a / nebo paměť) poté, co byly použité.
OTG-DS-008 - 4.9.8 Storing too Much Data in Session	Zkontrolovat, zda je možné přidělit velké množství dat do uživatelské relace, aby server vyčerpal své paměťové zdroje.

Testing for weak Cryptography (Testování slabé kryptografie)	
OTG-CRYPST-001 - 4.10.1 Testing for Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection	Testovat nedostatečnou sílu SSL/TLS
OTG-CRYPST-002 - 4.10.2 Testing for Padding Oracle	Testovat na chyby „Padding Oracle“ neboli funkce aplikace, která dešifruje zašifrované údaje poskytované klientem, např. stavy interní relace uložené v klientovi a úniku stavu platnosti funkce

	po dešifrování. Existence této zranitelnosti umožňuje útočníkovi dešifrovat šifrované data a šifrovat libovolná data bez znalosti klíčů použitého pro tyto kryptografické operace.
OTG-CRYPST-003 - 4.10.3 Testing for Sensitive information sent via unencrypted channels	Testovat na chyby zabezpečení přenosového kanálu, v kterém mohou být přenášeny informace v čistém textu. Zkontrolovat, zda jsou tyto informace přenášeny přes protokol HTTP namísto protokolu HTTPS nebo zda jsou používány slabé Cypher algoritmy.
OTG-CRYPST-004 - 4.10.4 Testing for Weak Encryption	Testovat na přítomnost slabých kryptokódů.

Business logic testing (Prověření logiky aplikace)	
OTG-BUSLOGIC-001 - 4.11.1 Testing for Business Logic data validation	Testovat na chyby v logice aplikace umožňující uživateli provést operaci s daty jiným způsobem než bylo navrženo.
OTG-BUSLOGIC-002 - 4.11.2 Test Ability to forge requests	Testovat zranitelnosti vůči využití proxy k odeslání žádostí HTTP POST / GET do aplikace Zkontrolujte projektovou dokumentaci a použijte průzkumné testování, které hledá odhadnutelnou, předvídatelnou nebo skrytou funkcionalitu polí.
OTG-BUSLOGIC-003 - 4.11.3 Test integrity checks	Testovat na chyby v zajištění integrity aplikace. Odolnost vůči nepovolenému odeslání hodnot skrytých polí serveru pomocí serveru proxy
OTG-BUSLOGIC-004 - 4.11.4 Test for Process Timing	Testovat na časové odezvy při nesprávném zadání autentifikačních údajů.
OTG-BUSLOGIC-005 - 4.11.5 Test number of times a function can be used limits	Zkontrolujte projektovou dokumentaci a použijte testování, které hledá funkce nebo funkce v aplikaci nebo systému, které by neměly být prováděny více než jednou nebo pouze určitým počtem opakování během pracovního postupu v aplikaci.
OTG-BUSLOGIC-006 - 4.11.6 Testing for the Circumvention of Work Flows	Testovat na chyby v logice aplikace umožňující uživateli provést operaci s daty jiným způsobem než bylo navrženo.
OTG-BUSLOGIC-007 - 4.11.7 Test defenses against application misuse	Testovat na přítomnost obranných mechanismů v aplikační vrstvě, které chrání aplikaci proti nesprávnému použití nebo neplatnému použití platné funkce, které se snaží kompromitovat webovou aplikaci, identifikovat slabé stránky a zneužívat zranitelnosti.
OTG-BUSLOGIC-008 - 4.11.8 Test Upload of Unexpected File Types	Testovat mechanismus ověřování správného typu souborů. Aplikace může očekávat, že budou na zpracovávány pouze určité typy souborů, jako jsou soubory .CSV, .txt. Aplikace musí ověřovat nahraný soubor buď podle přípony (pro ověření souboru s nízkou jistotou) nebo podle obsahu (ověření souboru s vysokou jistotou). To může vést k neočekávaným výsledkům systému nebo databáze v rámci aplikace / systému nebo k tomu, že útočníkům poskytnou další metody pro využití aplikace / systému.
OTG-BUSLOGIC-009 - 4.11.9 Test Upload of Malicious Files	Testovat na zranitelnost vůči škodlivým kódům.

Client Side Testing (Testování klienta)	
OTG-CLIENT-001 - 4.12.1 Testing for DOM-based Cross site scripting	Prověřit existenci DOM (document object model) XSS zranitelností.
OTG-CLIENT-002 - 4.10.2 Testing for JavaScript Execution	Otestovat provádění JAVA skriptů a ověřit, zda nelze získat osobní data uživatele nebo upravit obsah web stránky, kterou uživatel může vidět. Chyba zabezpečení typu JavaScript Injection je podtyp CrossScriptingu (XSS), který zahrnuje možnost

	vkládat libovolný kód JavaScript, který aplikace provádí uvnitř prohlížeče oběti.
OTG-CLIENT-003 - 4.12.3 Testing for HTML Injection	Prověřit odolnost vůči zranitelnosti typu HTML injection.
OTG-CLIENT-004 - 4.12.4 Testing for Client Side URL Redirect	Zkontrolovat odolnost aplikace, když aplikace přijímá nedůvěryhodný vstup, který obsahuje hodnotu URL, aniž by jej dezinfikoval. Odolnost vůči přesměrování webové aplikace na jinou stránku.
OTG-CLIENT-005 - 4.12.5 Testing for CSS Injection	Prověřit odolnost vůči zranitelnosti typu CSS Injection.
OTG-CLIENT-006 - 4.12.6 Testing for Client Side Resource Manipulation	Otestovat odolnost vůči zranitelnosti typu Client Side Resource Manipulation.
OTG-CLIENT-007 - 4.12.7 Test Cross Origin Resource Sharing	Prověřit používání CORS a otestovat, že není změněn Javascriptem. Otestovat protokoly na úrovni aplikace, že se používají k ochraně citlivých dat.
OTG-CLIENT-008 - 4.12.8 Testing for Cross site flashing	Prověřit existenci XSF (Cross Site Flashing) zranitelností.
OTG-CLIENT-009 - 4.12.9 Testing for Clickjacking	Otestovat odolnost vůči útokům typu Clickjacking
OTG-CLIENT-010 - 4.12.10 Testing WebSockets	Prověřit zda je webová služba přístupná přes HTTP a zda server ověřuje hlavičku Origin v počátečním handshake HTTP WebSocket. Pokud server neověřuje záhlaví původu v počátečním handshake serveru WebSocket, server WebSocket může přijímat připojení z libovolného původu.
OTG-CLIENT-011 - 4.10.12.11 Test Web Messaging	Je třeba provést ruční testování a kód JavaScript analyzovat hledáním implementace služby Web Messaging. Zejména je třeba prověřit, jak webové stránky omezují zprávy z nedůvěryhodné domény a jak se s nimi zachází i pro důvěryhodné domény
OTG-CLIENT-012 - 4.10.12 Test Local Storage	Prověřit existenci lokálního uložiště (Web Storage nebo Offline Storage), což je mechanismus pro ukládání dat jako párů klíč / hodnota svázaných s doménou a vynucených stejnou zásadou původu (SOP). Existují dva objekty, localStorage, který je trvalý a má uchovat data i po restartování prohlížeče / systému a sessionStorage, který je dočasný a bude existovat pouze dokud nebude okno nebo karta uzavřena.