Smlouva na Rozvoj a údržbu DMS v letech 2025 – 2030

č. sml. Zadavatele: ČÚZK-036829/2025

č. sml. Dodavatele: 009/2025

Smluvní strany:

Česká republika - Český úřad zeměměřický a katastrální

sídlo:	Pod sídlištěm 1800/9, Kobylisy, 182 11 Praha 8
IČO:	00025712
jejímž jménem jedná:	Ing. Radek Chromý, Ph.D., místopředseda

(dále jen „Zadavatel“)

a

CCA Group a.s.

Se sídlem:	Klimentská 1652/36, 110 00 Praha 1
Zastoupená:	Mgr. Barborou Barcalovou, MBA, předsedkyní představenstva
Zapsaná:	V OR vedeném Městským soudem v Praze, sp. značka B5556
IČO:	25695312
DIČ:	CZ25695312
ID DS:	8h6dcas

(dále jen „Dodavatel“)

u z a v í r a j í

tuto Smlouvu na rozvoj a údržbu DMS v letech 2025 - 2030 (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 2025 - 2030.

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 2025 - 2030“, Evid. číslo ve Věstníku veřejných zakázek: Z2025-013949, pro jejíž realizaci je tato Smlouva uzavírána.

1.6. ZD: Zadávací dokumentace VZ.

1.7. Součástí definic pojmů jsou i pojmy uvedené v Příloze S01 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 Dokument management systém v letech 2025 – 2030 (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. Na opakované služby rozvoje DMS budou smluvními stranami uzavírány objednávky, respektive dílčí smlouvy (dále jen „dílčí smlouvy“). Výstup plnění může mít povahu díla.

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 S06 této Smlouvy.

2.5.2. Rozvoj a údržba DMS na objednávku

- Další požadavky, neřešené v rámci paušálního poplatku, budou řešeny na základě dílčích smluv.
- 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 podporu při instalacích;
- 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 dílčí smlouvy a budou fakturovány na základě výkazů práce odsouhlasených a potvrzených Zadavatelem.

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 60 měsíců od prvního dne měsíce následujícího po účinnosti Smlouvy, nejdříve však od 1. 6. 2025.

3.2. Doba jednotlivých dílčích plnění bude definována v příslušných dílčích smlouvách.

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 S09 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 Dodavatele 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. Dodavatel se zavazuje udržovat v platnosti po celou dobu plnění závazků ze Smlouvy certifikáty a osvědčení stanovené v ZD, vztahující se k Dodavateli a osobám, které se budou podílet na provádění Smlouvy.

5.4. 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. V případě, že Zhotovitel využívá poddodavatele k výkonu činností vymezených v této Smlouvě, odpovídá za kvalitu, bezpečnost a včasnost plnění stejným způsobem, jako by činnost prováděl sám.

5.5. 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 Dodavatele 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.

5.6. Zadavatel v souladu s ustanovením § 6 odst. 4 ZZVZ, trvá na dodržování zásady sociálně odpovědného zadávání, environmentálně odpovědného zadávání a inovací ve smyslu daného zákona. S ohledem na charakter zakázky Zadavatel požaduje po Dodavateli plnění veškerých povinností vyplývajících z právních předpisů České republiky, zejména pak z předpisů pracovněprávních, předpisů z oblasti zaměstnanosti a bezpečnosti a ochrany zdraví při práci, a to zejména, nikoliv však výlučně, předpisy upravující mzdy zaměstnanců, pracovní dobu, dobu odpočinku mezi směnami, placené přesčasy, bezpečnost práce apod., a to vůči všem osobám, které se na plnění veřejné zakázky podílejí. Zadavatel také požaduje, aby Dodavatel sjednal a dodržoval se svými poddodavateli smluvní podmínky srovnatelné s podmínkami sjednanými ve Smlouvě a řádně a včas plnil finanční závazky svým poddodavatelům. Je-li to při plnění Smlouvy relevantní, zavazuje se Dodavatel také k ekologické likvidaci případného elektro a ostatního odpadu.

6. TECHNOLOGICKÁ INFRASTRUKTURA A VÝVOJOVÉ PROSTŘEDÍ DODAVATELE

6.1. Pro realizaci předmětu této Smlouvy se Dodavatel zavazuje mít k dispozici 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 ZD03 – Dokumentace DMS, 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 S08 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 svém 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. ZABEZPEČENÍ OCHRANY DAT DMS

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

9.2. S ohledem na to, že se Dodavatel stane významným dodavatelem dle zákona č. 181/2014 Sb. (ZoKB) a vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb. (VoKB)., musí při realizaci předmětu Smlouvy dodržovat Pravidla pro dodavatele - minimální bezpečnostní standard pro významné dodavatele, který je uveden v příloze smlouvy S05.

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

10. OCHRANA OSOBNÍCH ÚDAJŮ A DŮVĚRNÝCH INFORMACÍ

10.1. Ochrana osobních údajů bude realizována v souladu účinnou právní úpravou, tj. zejména se zákonem č. 110/2019 Sb., o zpracování osobních údajů, a Obecným nařízením o ochraně osobních údajů (GDPR - Nařízení Evropského parlamentu a Rady (EU) 2016/679), tak, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům při plnění předmětu této Smlouvy, k jejich zneužití, změně, zničení či ztrátě.

10.2. Dodavatel se zavazuje pro případ, že se v průběhu plnění předmětu této Smlouvy dostane do kontaktu s osobními údaji, že je bude ochraňovat a nakládat s nimi plně v souladu s příslušnými právními předpisy, a to i po ukončení plnění této Smlouvy. Smluvní strany se v případě, že se Dodavatel dostane do pozice zpracovatele osobních údajů ve správě Zadavatele, ve smyslu příslušných ustanovení zákona o ochraně osobních údajů zavazují uzavřít dodatek ke Smlouvě spočívající ve Smlouvě o zpracování osobních údajů. 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, neztratit či neznehodnotit.

10.3. Za důvěrné informace se bez ohledu na formu jejich zachycení považují ty informace, které jedna ze smluvních stran výslovně označila za důvěrné (dále jen „Důvěrné informace“).

10.4. Zadavatel považuje mimo jiné za důvěrné veškeré technické informace o jeho vnitřním prostředí a technické detaily týkající se jeho technické infrastruktury, které nejsou obecně známé.

10.5. Za Důvěrné informace Zadavatele se dále bezpodmínečně považují veškerá data, která DMS obsahuje, která do něj mají být, byla nebo budou Dodavatelem, Zadavatelem či třetími osobami vložena, a to i data, která z něj byla získána. Bez ohledu na ostatní ustanovení této Smlouvy jsou za Důvěrné informace Zadavatele považovány též zdrojové kódy DMS, jejichž poskytnutí třetí osobě by mohlo ohrozit bezpečnost dat Zadavatele v DMS.

10.6. Smluvní strany se zavazují, že během plnění Smlouvy i po jejím ukončení budou chránit Důvěrné informace druhé smluvní strany, o kterých se dozví od druhé smluvní strany v souvislosti s plněním Smlouvy, tak jako chrání svoje vlastní informace stejné důležitosti a budou ve vztahu k nim zachovávat mlčenlivost a nezpřístupní je třetí osobě. Smluvní strany se v této souvislosti zavazují poučit veškeré osoby, které se na jejich straně budou podílet na plnění této Smlouvy, o povinnosti mlčenlivosti a ochrany Důvěrných informací a dále se zavazují vhodným způsobem zajistit dodržování těchto povinností všemi osobami podílejícími se na plnění této Smlouvy.

10.7. Za třetí osoby se ve smyslu této Smlouvy nepovažují:

10.7.1. zaměstnanci smluvních stran a osoby v obdobném postavení,

10.7.2. poddodavatelé druhé smluvní strany za předpokladu, že se podílejí na plnění této Smlouvy nebo na plnění spojeném s plněním dle této Smlouvy, Důvěrné informace jsou jim zpřístupněny výhradně za tímto účelem a zpřístupnění Důvěrných informací je v rozsahu nezbytně nutném pro naplnění jeho účelu a za stejných podmínek, jaké jsou stanoveny smluvním stranám v této Smlouvě.

10.8. Bez ohledu na výše uvedená ustanovení se za Důvěrné informace nepovažují informace, které:

10.8.1. se staly veřejně známými, aniž by jejich zveřejněním došlo k porušení povinnosti druhé smluvní strany či právních předpisů;

10.8.2. měla druhá smluvní strana prokazatelně legálně k dispozici před uzavřením této Smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi smluvními stranami uzavřené smlouvy;

10.8.3. po podpisu této Smlouvy poskytne druhé smluvní straně třetí osoba, jež není omezena v takovém nakládání s informacemi;

10.8.4. je-li zpřístupnění informace vyžadováno zákonem či jiným právním předpisem včetně práva EU, soudem nebo oprávněným orgánem veřejné moci;

10.8.5. jsou obsažené v Smlouvě (ledaže podléhají výjimce z uveřejnění podle příslušných právních předpisů) anebo jsou zveřejněné na příslušných webových stránkách dle platné právní úpravy;

10.8.6. které jsou poskytnuty třetím stranám s předchozím souhlasem té smluvní strany, která informace označila za Důvěrné.

10.9. Veškeré Důvěrné informace zůstávají výhradním vlastnictvím předávající smluvní strany a přijímající smluvní strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní Důvěrné informace. S výjimkou rozsahu, který je nezbytný pro plnění této Smlouvy, se obě smluvní strany zavazují neduplikovat žádným způsobem Důvěrné informace druhé smluvní strany, nepředat je třetí osobě ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli plnit tuto Smlouvu. Smluvní strany se zároveň zavazují nepoužít Důvěrné informace druhé smluvní strany jinak než za účelem plnění této Smlouvy.

10.10. Veškerá data a provozní údaje zůstávají výhradním vlastnictvím Zadavatele, Dodavatel je s nimi oprávněn nakládat pouze v nezbytně nutném rozsahu, tj. neduplikovat je žádným způsobem, nepředat je třetí osobě ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli plnit tuto Smlouvu, a to pouze po nezbytně dlouhou dobu. Veškerá data, přihlašovací údaje do IT prostředí Zadavatele, provozní údaje a jakékoliv další údaje obdobného typu, včetně osobních údajů a případně dat, která jsou předmětem migrace dat, musí být Dodavatelem zlikvidována nejpozději s ukončením Smlouvy, nebude-li písemně dohodnuto jinak. Pravidla pro likvidaci dat jsou součástí bezpečnostní dokumentace.

10.11. Při plnění povinnosti vyplývající z této Smlouvy je Dodavatel povinen zajistit požadovanou úroveň ochrany důvěrnosti (např. formou NDA), integrity (např. šifrování dat, použití elektronického podpisu) a dostupnosti (např. formou SLA) alespoň na úrovni norem definovaných v bezpečnostní dokumentaci.

10.12. V případě, že jakékoliv plnění ze strany Dodavatele bude mít charakter utajovaných informací ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále je „ZBZ“), je Dodavatel povinen oznámit potřebu jakékoliv součinnosti v tomto směru dostatečně předem.

10.13. Dodavatel se dále zavazuje, že žádná neoprávněná osoba nezíská přístup k utajovaným informacím podle ZBZ. Dodavatel se také zavazuje zřetelně Zadavatele upozornit na skutečnost, že předávaný výstup obsahuje utajované informace a v jaké části výstupu je taková utajovaná informace uvedena.

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. Zadavatel po dobu plnění této Smlouvy umožní Dodavateli přístup prostřednictvím sítě internet k vývojovému prostředí a řízený přístup k testovacímu a produkčnímu prostředí souvisejícím s plněním Smlouvy. Přístup k produkčnímu prostředí bude Dodavatel využívat v minimálně nutném rozsahu pro naplnění účelu 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 testování 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 S09 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.11.18. Zástupci oprávněných osob přitom oprávněnou osobu zastupují při plnění její působnosti. Tím není dotčena možnost smluvních stran komunikovat prostřednictvím statutárních orgánů.

11.10. Zadavatel se zavazuje zajistit online dostupné zabezpečené úložiště pro vzájemnou výměnu dat s Dodavatelem. Úložiště bude např. sloužit pro objemnější data, která nelze přenést e-mailem (předávání dodávek, různé logy a výstupy apod.). Zadavatel se zavazuje zabezpečené úložiště plně zprovoznit nejpozději do 2 měsíců od začátku účinnosti Smlouvy.

11.11. Dodavatel se zavazuje zajistit vedení dokumentace projektových výstupů a projektové kanceláře (PK) v elektronické podobě. Dodavatel se zavazuje využívat PK Zadavatele, která je provozována na technologii Sharepoint online mimo interní prostředí Zadavatele. Dodavateli budou poskytnuty maximálně 4 přístupové licence Zadavatele, dále Dodavatel může využít své licence Office 365 v programu, který umožňuje přístup k použité službě. Přístupy Dodavateli budou umožněny na základě žádosti do 1 měsíce od začátku účinnosti Smlouvy. Podrobnosti jsou uvedeny v Příloze Smlouvy.

11.12. 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.17.4.1 a HelpDesku Dodavatele, s tím, že podrobnosti jsou uvedeny v Příloze S10 Smlouvy.

11.13. Součinnost smluvních stran při plnění této Smlouvy v oblasti testování nových verzí DMS bude realizována prostřednictvím SW nástroje Test, do kterého bude vhodným způsobem integrován, případně automatizovaně propojen, vlastní nástroj Dodavatele pro podporu / řízení testů, a to nejpozději do 6 měsíců od účinnosti Smlouvy.

11.14. Zadavatel dále požaduje, aby výstupy testovacích scénářů od Dodavatele byly v takovém formátu, aby bylo možné je do SpiraTest importovat pomocí doplňku MS Excel – SpiraExcelAddIn (aktuální verze SpiraTest Verze v7.13.0.0).

11.15. Oprávněné osoby podle této Smlouvy jsou oprávněny zastupovat smluvní stranu při plnění této Smlouvy a při jednáních souvisejících s přípravou dílčích smluv 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.

11.16. Všechny dokumenty, mající vztah k plnění této Smlouvy, musí být podepsány oprávněnými osobami obou smluvních stran nebo jejich zástupci. Komunikace smluvních stran probíhá na úrovni oprávněných osob, zástupci Hlavních oprávněných osob přitom Hlavní oprávněnou osobu v době její nepřítomnosti zastupují při plnění její působnosti. Tím není dotčena možnost smluvních stran komunikovat prostřednictvím statutárních orgánů. Konkrétní okruh působnosti jednotlivých oprávněných osob bude stanoven dohodou smluvních stran. V pochybnosti se má za to, že oprávněna k činění úkonu je Hlavní oprávněná osoba.

11.17. Do působnosti oprávněných osob náleží:

11.17.1. kontrolovat postup plnění této Smlouvy a dílčích smluv;

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

11.17.3. organizačně zabezpečovat veškeré činnosti související s plněním této Smlouvy a dílčích smluv;

11.17.4. koordinovat součinnost smluvních stran;

11.17.5. informovat na vyžádání smluvní strany o postupu plnění této Smlouvy a dílčích smluv.

11.18. Oprávněnými osobami jsou:

	Zadavatel	Dodavatel
Oprávněné osoby	[redacted]	[redacted]
Zástupci oprávněných osob	[redacted]	[redacted]

11.19. 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.

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

11.20.1. osobně oproti potvrzení o převzetí;

11.20.2. do datové schránky příjemce;

11.20.3. 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;

11.20.4. 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;

11.20.5. finalizací dokumentu v PK. V tomto případě se dokumenty považují za podepsané a doručené v okamžiku, kdy Oprávněná osoba protistrany elektronickou poštou potvrdila protistraně, že předaný dokument je pro ni v PK dostupný.

12. PŘEBÍRÁNÍ VÝSTUPŮ, AKCEPTAČNÍ ŘÍZENÍ

12.1. 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.

12.2. 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.

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

12.3.1. **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.

12.3.2. **Akceptováno s výhradami**. V případě, že budou v průběhu akceptačního řízení zjištěny v předaném plnění vady nebo nedodělky, nebránící dalšímu užití plnění, 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 12.4. V případě, že Dodavatel neodstraní/nedořeší vady a nedodělky ve stanoveném termínu, bude Zadavatel požadovat slevu z ceny plnění, viz ustanovení níže.

12.3.3. **Neakceptováno**. V případě, že budou v průběhu akceptačního řízení v předaném plnění zjištěny takové vady a nedodělky, které by bránily v užití plnění 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.

12.4. 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:

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

12.4.2. 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 termínu 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. 12.1 a 12.2 Smlouvy. Měsícem se p rozumí 30 kalendářních dní. Minimální snížení Doplatku přitom činí 10 % z výše Doplatku.

12.4.3. 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 12.4.2.

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

12.5.1. výstupní protokol z interního testování na straně Dodavatele,

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

12.5.3. 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,

12.5.4. uživatelskou příručku,

12.5.5. administrátorskou uživatelskou příručku,

12.5.6. instalační příručku,

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

12.5.8. provozní dokumentaci,

12.5.9. dokumentaci pro školení.

12.6. 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:

12.6.1. 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,

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

12.6.3. 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,

12.6.4. programátorskou dokumentaci,

12.6.5. uživatelskou příručku,

12.6.6. administrátorskou uživatelskou příručku,

12.6.7. instalační příručku,

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

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

12.6.10. výsledky bezpečnostních testů a provedení kontrolních checklistů,

12.6.11. dotčená (změněná) provozní dokumentace,

12.6.12. systémová příručka IS,

12.6.13. dokumentace pro školení.

13. CENA PLNĚNÍ

13.1. Celková maximální cena plnění podle této Smlouvy činí 66 500 000,- Kč bez DPH. Celková cena bude hrazena v průběhu plnění této Smlouvy za jednotlivá plnění podle této Smlouvy a dílčích smluv.

13.2. Jednotkové ceny resp. jednotlivé položky činí:

Položka	Plnění	Jednotka	Celková cena v Kč bez DPH
1	Rozvoj a údržba na objednávku	1 ČLD	8.500 Kč
2	Průběžný rozvoj, bezpečnost a údržba	1 kalendářní měsíc	955.000 Kč

13.3. 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.

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

14. PLATEBNÍ A FAKTURAČNÍ PODMÍNKY

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

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

14.3. 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. dílčí smlouvy přidělené Zadavatelem. Společně s fakturami Dodavatel poskytne elektronické originály, či listinné 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 musí být přiložen schválený akceptační protokol.

14.4. Pro jednotlivé části plnění ve smyslu odst.13.2. jsou platné navíc tyto specifické platební podmínky:

14.4.1. Pro fakturaci cen podle odst.13.2., 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.13.2., položky 1 akceptovat potvrzením měsíčního výkazu práce, přičemž fakturačním obdobím bude ukončené čtvrtletí v rámci plnění Smlouvy. Fakturu na úhradu prací na základě dílčí smlouvy 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.

14.4.2. Pro fakturaci ceny podle odst. 13.2 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.

14.5. Faktura je splatná do 21 kalendářních dnů ode dne jejího doručení Zadavateli, a to do datové schránky Objednatele, ID: uuaaatg nebo cuzk@cuzk.gov.cz. V případě nutnosti v tištěné podobě (ve dvou vyhotoveních) na adresu: Pod sídlištěm 1800/9, Kobylisy, 18211 Praha 8. V případě předložení faktury v období od 15. prosince do 31. ledna bude splatnost faktury stanovena na 30 dnů ode dne doručení Zadavateli.

14.6. 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 smlouvě s tím, že doba splatnosti nové (opravené) faktury začíná znovu běžet ode dne jejího doručení Zadavateli.

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

14.8. Zadavatel neposkytuje zálohové platby.

15. PRÁVA A POVINNOSTI SMLUVNÍCH STRAN

15.1. 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.

15.2. 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.

15.3. 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.

15.4. 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.

15.5. Dodavatel se zavazuje, že pro plnění realizované na základě dílčích smluv 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.

15.6. Dodavatel se zavazuje, že pro plnění realizované na základě dílčích smluv 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).

15.7. 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.

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

15.9. 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, nástrojům, dokumentaci a dalším podkladům a výstupům souvisejícím s plněním) v rozsahu nezbytném pro řádné plnění této Smlouvy.

15.10. 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:

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

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

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

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

15.11. 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.

15.12. 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.

15.13. Dodavatele se zavazuje, že pokud budou v rámci plnění této Smlouvy dodány licence SW nad rámec stávajícího stavu, že provozování daného SW v rámci TI Zadavatele nebude porušovat pravidla definovaná výrobcem daného SW a bude s nimi v souladu.

15.14. Dodavatel je povinen Zadavatele předem informovat o významné změně ovládání Dodavatele. Ovládáním se zde rozumí zejména ovládání či řízení podle § 74 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, či ekvivalentní postavení. Notifikační povinnost je taktéž navázána na změnu skutečného majitele v evidenci skutečných majitelů (§ 118b a násl. zákona č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob a o evidenci svěřenských fondů). Zadavatel je povinen bez zbytečného odkladu sdělit své stanovisko ohledně svého záměru dále pokračovat či nepokračovat ve smluvním vztahu založeném touto Smlouvou i po změně ovládání Dodavatele.

15.15. Uplatní-li třetí osoba vůči Zadavateli před soudem nebo mimo soud jakékoli své nároky k předmětu plnění či jeho části (zejména v oblasti práv duševního vlastnictví, jako například patentových a autorských práv a obchodních značek), Dodavatel bude Zadavatele před těmito nároky bránit a důvodné nároky třetí osoby na vlastní náklady bez zbytečného odkladu vypořádá, případně poskytne na vlastní náklady právní servis/zastupování v obvyklé výši pro Zadavatele při jeho obraně. Vypořádání, právní servis/zastupování bude poskytnuto v případě, že Dodavatel bude neprodleně písemně informován Zadavatelem o nároku uplatněném třetí stranou a budou mu ze strany Zadavatele poskytnuty potřebné informace a součinnost. Dodavatel se také zavazuje v této souvislosti uhradit veškeré škody, pokuty, náklady apod., které bude Zadavatel povinen v důsledku výše uvedeného uhradit.

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

15.17. 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.

15.18. 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.

15.19. 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.

15.20. 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.

15.21. 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.

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

16. VYŠŠÍ MOC

16.1. Žádná ze smluvních stran nebude považována za odpovědnou za nesplnění některého ustanovení této Smlouvy, budou-li příčinou nepředvídatelné, neodvratitelné a povinnou stranou nekontrolovatelné okolnosti nebo události, které způsobují, že plnění povinností není možné nebo je krajně obtížné. Za vyšší moc se považují zejména epidemie, ozbrojené konflikty, přírodní katastrofy (dále též jako „vyšší moc“).

16.2. Smluvní strana, která porušuje svou povinnost nebo která s přihlédnutím ke všem okolnostem má vědět, že poruší svou povinnost založenou touto Smlouvy, nebo která se dozví o okolnosti vyšší moci, bránící plnění povinnosti dle této Smlouvy, je povinna oznámit písemně druhé smluvní straně povahu překážky, která jí brání nebo bude bránit v plnění povinnosti, a o jejích důsledcích. Zpráva musí být podána bez zbytečného odkladu, nejpozději však do 5 pracovních dnů poté, kdy se povinná smluvní strana o překážce dověděla nebo při náležité péči mohla dovědět. Druhá smluvní strana je povinna přijetí takové zprávy bez zbytečného odkladu písemně potvrdit. Stejným způsobem musí být obeznámena druhá smluvní strana o ukončení překážky bránící splnění povinností vyplývajících z této Smlouvy.

17. ZÁRUKA, PODMÍNKY ZÁRUČNÍ PODPORY

17.1. Dodavatel garantuje, že DMS bude fungovat v souladu s touto Smlouvou a ZD. Dodavatel přebírá závazek odstranit na své náklady vady díla, které se vyskytnou v průběhu záruční doby.

17.2. 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.

17.3. Záruka:

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

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

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

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

17.5. Detailní popis záruky a podmínek záruční podpory je uveden v Příloze S07 Smlouvy.

17.6. 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.

17.7. 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.

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

18.1. 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.

18.2. 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.

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

18.4. Dodavatel prohlašuje, že jím poskytované plnění bude odpovídat všem požadavkům vyplývajícím z účinných 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.

18.5. Dodavatel není v prodlení, pokud je prodlení způsobeno neposkytnutím dohodnuté součinnosti Zadavatelem.

18.6. 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.

18.7. Dodavatel se zavazuje v případě prodlení s plněním poskytnout Zadavateli slevu z ceny plnění ve výši 0,5 % z celkové ceny příslušného plnění (např. dílčí smlouvy; 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.

18.8. 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.

18.9. Dodavatel se zavazuje pro případ nesplnění garantované úrovně záručního servisu poskytnout Zadavateli slevu z ceny ve výši 5.000,- Kč za každou započatou hodinu resp. den nedodržení SLA, a to z ceny průběžného rozvoje, bezpečnosti a údržby DMS.

18.10. 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.

18.11. 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.

18.12. 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.

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

18.14. 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.

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

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

18.17. 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.

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

19. PRAVIDLA PRO UPŘESŇOVÁNÍ ROZSAHU PLNĚNÍ DÍLČÍMI SMLOUVAMI

19.1. Smluvní strany mohou uzavírat dílčí smlouvy, na základě kterých bude upřesňován předmět plnění podle čl.2.5.2.

19.2. Dílčí smlouvy budou uzavírány jako smlouvy o dílo v souladu ustanoveními § 2586 a násl. občanského zákoníku. Bude-li součástí dílčí smlouvy 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 dílčí smlouvy 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 dílčí smlouvy jako funkční dílo.

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

19.4. Ukončení účinnosti kterékoliv dílčí smlouvy nemá vliv na platnost ani účinnost této Smlouvy.

20. MOŽNOSTI ODSTOUPENÍ OD SMLOUVY A VÝPOVĚDI SMLOUVY

20.1. Účinnost této Smlouvy lze předčasně ukončit:

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

20.1.2. ze strany Zadavatele písemným odstoupením od Smlouvy či dílčí smlouvy 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 dílčí smlouvy 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 dílčí smlouvy 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.

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

20.1.4. 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.

20.1.5. ze strany Zadavatele odstoupením od této Smlouvy v případě významné změny kontroly Dodavatele s tím, že změnou kontroly Dodavatele se rozumí změna ovládání či řízení podle § 74 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, změna vlastnictví zásadních aktiv, popřípadě změna oprávnění nakládat s těmito aktivy, využívanými Dodavatelem k plnění Smlouvy.

20.2. 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).

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

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

21.1.1. kompletní zdrojové kódy;

21.1.2. skripty pro generování databázových schémat;

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

21.1.4. export repository pro Enterprise Architect;

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

21.1.6. principy monitorování a aktualizace požadavků;

21.1.7. stávající bezpečnostní dokumentace;

21.1.8. systémová příručka IS.

21.2. Dodavatel se zavazuje, že nepoužije výstupy dle čl. 21.1. 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.

21.3. 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.

21.4. Pro případy, že součástí plnění 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 (dále jen „autorský zákon“), poskytuje Dodavatel Zadavateli oprávnění k výkonu práva autorské dílo užít (dále jen „licenci“) v dále specifikovaném rozsahu.

21.5. V případě, že takové autorské dílo či jeho část (dále jen „dílo“) je výsledkem činnosti dle této Smlouvy resp. dílčí smlouvy, tj. bude zhotoveno Dodavatelem případně poddodavatelem Dodavatele pro účely splnění této Smlouvy (dále jen „SW vytvořený pro Smlouvu“), uděluje Dodavatel Zadavateli licenci specifikovanou níže:

21.5.1. 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;

21.5.2. neomezený územní či množstevní rozsah licence;

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

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

21.5.5. licenci není Zadavatel povinen využít.

21.5.6. Podle ustanovení § 12 odst. 4 autorského zákona je Zadavatel oprávněn ke všem způsobům užití díla 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 instalačních souborů, struktury a popisu databáze, vývojové, bezpečnostní, provozní a uživatelské dokumentace a to tak, že budou uloženy na k tomu vyhrazených datových prostředcích Zadavatele nebo mu budou nejpozději k datu předání plnění nebo jeho části předány na datovém nosiči. Zdrojovým kódem se rozumí zápis textu počítačového programu v některém programovacím jazyce. Zdrojové kódy musí být předávány konzistentní, bez chyb, kompletní, ve správné verzi, zaručující ověření v prostředí zadavatele, kompilaci, sestavení, instalaci, spuštění a ověření funkcionality.

21.6. Součástí plnění resp. díla může být tzv. proprietární software (dále jen „proprietární software“), u kterého Dodavatel nemůže udělit Zadavateli oprávnění dle předchozích ustanovení nebo to po něm nelze spravedlivě požadovat, nicméně pouze při splnění některé z následujících podmínek:

21.6.1. Jedná se o software renomovaných výrobců, jenž je na trhu běžně dostupný, tj. nabízený na území České republiky alespoň třemi na sobě nezávislými a vzájemně nepropojenými subjekty oprávněnými takovýto software dodat, a který je v době uzavření Smlouvy/dílčí smlouvy prokazatelně užíván v produkčním prostředí nejméně u deseti na sobě nezávislých a vzájemně nepropojených subjektů. Dodavatel je povinen poskytnout Zadavateli o této skutečnosti písemné prohlášení a na výzvu Zadavatele tuto skutečnost prokázat.

21.6.2. Jedná se o software, u kterého Dodavatel poskytne s ohledem na jeho (i) marginální význam, (ii) nekomplikovanou propojitelnost či (iii) oddělitelnost a nahraditelnost bez nutnosti vynakládání výraznějších prostředků v rámci plnění dle

této Smlouvy, písemnou garanci, že další rozvoj DMS či jeho jakékoliv části jinou osobou než Dodavatelem je možné provádět bez toho, aby tím byla dotčena práva autorů takovéhoto softwaru, neboť nebude nutné zasahovat do zdrojových kódů takovéhoto softwaru anebo proto, že případné nahrazení takovéhoto softwaru nebude představovat výraznější komplikaci a náklad na straně Zadavatele. Dodavatel je povinen poskytnout Zadavateli o této skutečnosti písemné prohlášení a na výzvu Zadavatele tuto skutečnost prokázat.

21.6.3. Dodavatel Zadavateli k software poskytne nebo zprostředkuje poskytnutí úplných komentovaných zdrojových kódů software a bezpodmínečného práva provádět jakékoliv modifikace, úpravy, změny takového software a dle svého uvážení do něj zasahovat, zapracovávat ho do dalších autorských děl, zařazovat ho do děl souborných či do databází apod., a to i prostřednictvím třetích osob. Poskytování zdrojových kódů se pak řídí čl. 21.5.6

21.7. Pokud se bude jednat o proprietární software Dodavatele nebo třetích stran, tak na rozdíl od licence k SW vytvořenému pro Smlouvu postačí, aby udělená licence k takovému software zahrnovala nevýhradní oprávnění užít jej jakýmkoli způsobem nejméně po dobu trvání této Smlouvy, na území České republiky a v množstevním rozsahu, který je nezbytný pro pokrytí potřeb Zadavatele. V případě výpovědi či odstoupení od Smlouvy/dílčí smlouvy se Dodavatel zavazuje nabídnout Zadavateli právo užívat takovýto proprietární software v rozsahu, v jakém je to nezbytné pro řádné užívání díla. Tím není dotčeno právo Zadavatele pořídit takovýto software i od třetí osoby bez ohledu na licence pořízené dříve Dodavatelem. V případě využití tohoto přednostního práva se Dodavatel zavazuje, že právo užívat takovýto software dle tohoto odstavce Smlouvy nabídne Zadavateli za běžných tržních podmínek a bude vycházet z účetní hodnoty licencí, které pořídil. Dodavatel je povinen dokumentovat veškeré využití proprietárního software v rámci plnění dle této Smlouvy.

21.8. Nelze-li to po Dodavateli spravedlivě požadovat a není-li to v rozporu s ustanoveními o proprietárním software, nemusí být Zadavateli k proprietárnímu softwaru předány zdrojové kódy a stejně tak nemusí být poskytnuto právo Zadavatele do proprietárního softwaru zasahovat, vždy však musí být předána kompletní uživatelská, administrátorská a provozní dokumentace.

21.9. Jestliže jsou s užitím proprietárního software, služeb podpory k němu, či jiných souvisejících plnění spojeny jednorázové či pravidelné poplatky, je Dodavatel povinen v rámci ceny plnění uhradit všechny tyto poplatky za celou dobu trvání Smlouvy.

21.10. Je-li součástí plnění tzv. open source software, je Dodavatel povinen zajistit, aby se jednalo o open source software, který:

21.10.1. je veřejnosti poskytován zdarma, včetně detailně komentovaných zdrojových kódů, úplné uživatelské, provozní a administrátorské dokumentace a práva takový software měnit a současně je povinen zajistit, že právo Zadavatele takový open source užít (např. licence) a způsob jeho použití nesmí kontaminovat zdrojový kód jakékoliv části plnění dle Smlouvy, které jsou počítačovým programem, povinností jejich zveřejnění jakékoliv třetí straně; a současně

21.10.2. je na trhu běžně dostupný, tedy nabízený a podporovaný na území Evropské unie, Evropského hospodářského prostoru nebo Švýcarské konfederace alespoň třemi na sobě nezávislými a vzájemně nepropojenými osobami a současně je splněna nejméně jedna z níže uvedených podmínek:

a) v době uzavření této Smlouvy / dílčí smlouvy je prokazatelně užíván v produktivním prostředí nejméně u deseti subjektů; nebo

b) se jedná o open source software prokazatelně dostupný na trhu nejméně 3 roky, je průběžně aktualizován a počet jeho stažení za celou dobu dostupnosti na trhu činí nejméně 100.000;

21.10.3. a současně další rozvoj DMS nebo jeho části jinou osobou než

Dodavatelem je možné provádět bez omezení i při využití takovéhoto software.

21.11. Dodavatel je povinen poskytnout Zadavateli písemné prohlášení o splnění podmínek pro použití open source software a na výzvu Zadavatele tvrzené skutečnosti prokázat. Dodavatel je povinen dokumentovat veškeré využití open source software v rámci plnění dle Smlouvy.

21.12. Dodavatel je oprávněn při plnění dle této Smlouvy použít také proprietární, anebo nekomerční/open source software, jejichž využití při plnění Smlouvy dopředu nepředpokládal a neuvedl je proto ve své nabídce v ZŘ. Takovéto použití je však vždy podmíněno schválením ze strany Zadavatele.

21.13. V případě použití open source software nesmí být použit takový, který by začleněním do díla způsobil, že by dílo ztratilo svůj proprietární charakter (tj. jestliže by podle licenčních podmínek takového open source software jeho začleněním do díla došlo k povinnosti zpřístupnit jakoukoliv část díla pod tzv. svobodnou licenci/licencí copyleft).

21.14. Dodavatel prohlašuje, že vlastní veškerá oprávnění k dílu, 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 postoupení práva výkonu majetkových práv autorských). K tomu smluvní strany prohlašují, že pokud při poskytnutí plnění dle Smlouvy vznikne činností Dodavatele a Zadavatele dílo spoluautorů, bude se mít za to, že je Zadavatel oprávněn vykonávat majetková autorská práva k dílu spoluautorů tak, aby byl jejich výlučným vykonatelem a Dodavatel udělil Zadavateli souhlas k jakékoliv změně nebo jinému zásahu do díla spoluautorů.

21.15. Pokud bude výsledkem nebo součástí plnění dle Smlouvy databáze, která splňuje znaky autorského díla dle autorského zákona, poskytne Dodavatel Zadavateli k databázi shodná oprávnění jako k jakémukoliv jinému dílu dle této Smlouvy. Současně je Zadavatel v postavení pořizovatele databáze ve smyslu § 88 autorského zákona, což pro vyloučení jakýchkoliv pochybností rovněž zahrnuje i právo na vytěžování nebo zužitkování nebo zveřejnění (poskytnutí) databáze třetím osobám nebo k využití celého obsahu databáze nebo její kvalitativně nebo kvantitativně podstatné části. Dodavatel není oprávněn databázi bez souhlasu Zadavatele užívat.

21.16. Dodavatel prohlašuje, že užitím díla 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.

21.17. Odměna za veškerá oprávnění poskytnutá Zadavateli dle Smlouvy/dílčí smlouvy je již zahrnuta v ceně plnění dle této Smlouvy/dílčí smlouvy. Cena plnění obsahuje všechny licenční odměny, které mohou při plnění z této Smlouvy/dílčí smlouvy vzniknout. Dodavatel není oprávněn uplatňovat další licenční poplatky s ohledem na způsob použití licencí a charakteristiku prostředí, ve kterém jsou užívány. Smluvní strany mají za to, že je tímto odměna za licence ujednána, resp. je sjednán způsob jejího určení dostatečným způsobem s ohledem na ustanovení § 2366 občanského zákoníku. V ceně plnění dle Smlouvy/dílčí smlouvy jsou zahrnuty i všechny případné poplatky, které jsou spojeny s užitím proprietárního software, služeb podpory k němu, či jiných souvisejících plnění.

21.18. Udělení veškerých práv uvedených v čl. 21 nelze ze strany Dodavatele vypovědět a rovněž tak na udělení takových práv nemá vliv ukončení platnosti této Smlouvy/dílčí smlouvy. S ohledem na skutečnost, že licenční ujednání jsou sjednána na dobu určitou, smluvní strany si sjednávají, že Dodavatel není oprávněn učinit výpověď licenční smlouvy.

21.19. Dodavatel se zavazuje, že jakákoli Dodavatelem dodaná nebo zpřístupněná aktualizace, nebo jiná úprava je autorskoprávně nezávadná dle této Smlouvy a podléhá stejné licenci, jako je uvedená v této Smlouvě.

21.20. Dodavatel touto Smlouvou poskytuje Zadavateli licenci k dílu, přičemž účinnost této licence nastává okamžikem podepsání akceptačního protokolu s výsledkem „akceptováno“, tj. dnem, který je uveden v akceptačním protokolu; do té doby je Zadavatel oprávněn dílo užít v rozsahu a způsobem nezbytným k provedení akceptace předmětu plnění.

21.21. Licence se vztahuje též na zdrojové a strojové kódy i koncepční či jiné materiály, pokud mají být tyto zdrojové kódy a koncepční či jiné materiály dle této Smlouvy předány k užití Zadavateli dle této Smlouvy (včetně případných změn a nových verzí předaných Zadavateli).

21.22. Smluvní strany prohlašují, že pokud nastanou pochybnosti o rozsahu práv Zadavatele k předmětu Smlouvy, a to i kdykoliv v budoucnu, budou všechna ustanovení této Smlouvy a jejích příloh vykládána s ohledem na účel a cíle Smlouvy a vůli smluvních stran poskytnout Zadavateli takový předmět Smlouvy, u něhož není dán vendor lock-in, s kterým může Zadavatel volně nakládat, zejména ho jakkoliv modifikovat, upravovat, měnit, zasahovat do něj, a to i prostřednictvím třetích osob, aniž by mu v tom bránily jakékoliv právní překážky nebo překážky neprávní (např. nedostatečná dokumentace či zdrojové kódy či nedostatek součinnosti Dodavatele zejména při ukončení Smlouvy).

22. KOORDINACE S DALŠÍMI PROJEKTY ZADAVATELE

22.1. 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.

22.2. 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 solutions, s.r.o., Kentico Software s.r.o., Sefira spol. s.r.o., Microsoft s.r.o., Software602 a.s., a to za podmínky, že Zadavatel zajistí požadovanou spolupráci těchto dodavatelů s Dodavatelem.

22.3. 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.13.2, položce 1.

23. JINÁ USTANOVENÍ

23.1. 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.

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

23.3. 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.

23.4. 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.

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

23.6. Jednacím jazykem mezi Objednatelem a Zhotovitelem bude pro veškerá plnění vyplývající ze Smlouvy jazyk český nebo slovenský. Dokumentace bude vyhotovena výhradně v českém jazyce.

24. ZÁVĚREČNÉ USTANOVENÍ

24.1. Smlouva nabývá platnosti dnem jejího podpisu poslední ze smluvních stran.

24.2. Smluvní strany berou na vědomí, že tato Smlouva i dílčí smlouvy podléhají zveřejnění dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Smlouva i dílčí smlouvy nabudou účinnosti nejdříve dnem zveřejnění v registru smluv, nejsou-li pro nabytí účinnosti stanoveny další podmínky. Zveřejnění v registru smluv zajistí Objednatel a bezodkladně o něm informuje Zhotovitele.

24.3. Ukončením účinnosti této Smlouvy/dílčí smlouvy nejsou dotčena ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po zániku účinnosti této Smlouvy/dílčí smlouvy zejména ustanovení upravující práva duševního vlastnictví, ustanovení upravující ochranu Důvěrných informací, dále ustanovení upravující zpracování osobních údajů, ustanovení upravující zajištění bezpečnosti, sankce.

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

24.5. Nedílnou součástí této Smlouvy jsou přílohy:

Číslo Přílohy Smlouvy	Obsah přílohy Smlouvy
1	Seznam použitých pojmů a zkratek
2	Projektová kancelář
3	Práva a povinnosti manažera kybernetické bezpečnosti IS KII/VIS
4	Pravidla a způsob provádění bezpečnostních testů
5	Pravidla pro Dodavatele - minimální bezpečnostní standard pro významné dodavatele
6	Průběžný rozvoj, bezpečnost a údržba DMS
7	Záruka
8	Podrobný popis metodiky vývoje
9	Požadavky na způsob řízení projektu a personální zajištění Smlouvy
10	Propojení HD Zadavatele s HD Dodavatele

Datum: dle elektronického podpisu
Za Zadavatele:

Podpis: Viditelný elektronický podpis
Jméno: Ing. Radek Chromý, Ph.D.
Funkce: místopředseda ČÚZK

Datum: dle elektronického podpisu
Za Dodavatele:

Podpis: Viditelný elektronický podpis
Jméno: Mgr. Barbora Barcalová, MBA
Funkce: předsedkyně představenstva

Příloha S01 - Seznam 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
ČLH	Člověkohodina, tj. 60 minut práce jedné osoby (8 ČLH = 1 ČLD)
ČSN	Chráněné označení českých technických norem
ČÚZK	Český úřad zeměměřický a katastrální
DB	databáze
DMS	Dokument Management Systém
DPKN	Dálkový přístup, www rozhraní ISKN pro externí uživatele
DPN	Dálkový přístup pro neregistrované
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
IE	Internet Explorer
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
JAVA	Objektově orientovaný programovací jazyk
K	Záložní lokalita (serverovna ČÚZK)
KESSL	Komplexní elektronická spisová služba
KIVS	Komunikační infrastruktura veřejné správy
KN	Katastr nemovitostí
KP	Katastrální pracoviště
MTOM	Message Transmission Optimization Mechanism
NBD	Next business day (Další pracovní den)
NDKN	Nahlížení do katastru nemovitostí

.NET	Microsoft Net Framework
OB-TA	Obelisk trusted archive
PDF	Portable Document Format (Přenosný formát dokumentů)
PK	Projektová kancelář
PP	Produktová podpora
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
T	Primární lokalita (externí serverovna v Praze)
tel.	Telefon
TI	Technologická infrastruktura
TP	Technická podpora
VM	Vzdálený monitoring
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 – Webové stránky resortu
XML	eXtensible Markup Language, rozšiřitelný značkovací jazyk pro tvorbu strukturovaných dat
ZD	Zadávací dokumentace Veřejné zakázky „Rozvoj a údržba DMS v letech 2025 – 2030“
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 S02 - Projektová kancelář

Obsah

1. Úvod

1.1 Rozsah a určení dokumentu

Dokument obsahuje principy a způsob vedení projektové kanceláře (PK) v elektronické podobě.

Pojmem „Dokument“ se myslí obecný soubor v jednom z povolených formátů pro PK.

Seznam uživatelů ze strany Zadavatele a Dodavatele a jejich zařazení do rolí (viz dále) bude sestaven po zahájení účinnosti Smlouvy.

1.2 Přehled použitých zkratek a pojmů

Pojem	Vysvětlení
major/minor verze	Konvence ve verzování dokumentu v rámci PK (ne aplikace), kdy je verze tvořena 2 částmi: <major>(hlavní).<minor>(vedlejší). Např. „1.1“ nebo „2.0“
MS SHP	Microsoft Sharepoint Online
PK	Projektová kancelář
TI	Technologická infrastruktura Zadavatele

2. Použití PK

PK slouží k řízenému ukládání dokumentace projektu - dokumentů, které představují plnění a výstupy projektu dle Smlouvy a slouží ke komunikaci a ukládání důležitých skutečností (informace a dokumenty) projektu. Prostředí PK bude sloužit i jako online dostupné zabezpečené úložiště pro vzájemnou výměnu objemných dat.

Pro práci s projektovými dokumenty budou využívány nástroje ze sady Microsoft Office 2016. Pro dokumenty, které v rámci projektu nebudou upravovány nebo připomínkovány, lze po dohodě používat i jiné formáty (např. PDF, TXT apod.).

2.1 Řízení dokumentace

Vedoucí projektu Zadavatele odpovídá za řízení dokumentace projektu. Zejména se jedná o následující dokumenty:

- Sběr požadavků (SP) a Změnové požadavky (CR),
- Zápisy z jednání, především z jednání Řídícího výboru a Výkonného výboru,
- Zprávy o vývoji projektu,
- Akceptační protokoly a Zprávy o akceptaci,
- Bezpečnostní dokumentace,
- Klíčové výstupy z projektu,
- Schválené postupy a standardy,
- Uživatelská dokumentace,
- Technologické dokumenty (instalace, konfigurace apod.).

Všechny dokumenty projektu budou k dispozici účastníkům projektu v elektronické formě v PK. Přístup bude řešen pomocí nepřetržitého on-line zabezpečeného vzdáleného přístupu. Dostupnost dokumentů, v závislosti na stupni jejich ochrany, bude dána zařazením uživatelů do skupin a definovaným přístupem pro danou skupinu.

Do PK se vkládají dokumenty tak, aby bylo umožněno jejich verzování a sledování historie.

Schválení dokumentu (povýšení na hlavní verzi „1.0“, „2.0“ apod.) musí potvrdit Zadavatel i Dodavatel. Výsledné schválení do verze „1.0“, „2.0“ apod. provádí oprávněný zástupce Zadavatele.

2.2 Projektová kancelář – základní principy

Pro ukládání řízených projektových dokumentů je použit nástroj Microsoft SharePoint Online (MS SHP) provozovaný Zadavatelem.

- Za provoz PK odpovídá Zadavatel.
- Dokumenty budou uloženy ve struktuře složek s rozdělením dokumentů podle logických kategorií.
- Dokumenty budou verzovány prostředky nástroje MS SHP. Verze, které nejsou čistou „major verzí“ jako je „1.0“, „2.0“ apod. se považují za pracovní verze. Jde o verze „0.1“, „0.2“ nebo „1.1“, „1.3“ apod.
- Dokumenty budou identifikovány a jednotně pojmenovávány identifikací kategorie dokumentu, pořadovým číslem v rámci kategorie, názvem dokumentu korespondujícím s obsahem, případně rokem, měsícem a dnem pokud se jedná o zápis z porady. Ostatní údaje dokumentu jsou vedeny jako metadata na MS SHP (např. verze).
- Dokumenty budou přístupné určeným pracovníkům Zadavatele a Dodavatele dle jejich rolí. Uživatelské účty zřizuje a přístupová práva přiděluje určená odpovědná osoba Zadavatele dle odsouhlaseného seznamu uživatelů.

- PK bude přístupná prostřednictvím sítě internet.
- Autentizace a autorizace bude řešena prostřednictvím Microsoft Azure AD (Zadavatel nebude pro Dodavatele vytvářet účty ve své Azure AD, pouze přidělí oprávnění existujícím účtům z AD Dodavatele).
- V rámci PK je umožněno fulltextové vyhledávání.
- PK umožňuje logování a audit činností.
- PK umožňuje rezervaci dokumentů.
- PK umožňuje uložení různých typů dokumentů (Word, Excel, MS Project, ZIP, RAR apod.)
- PK umožňuje definovat rezervace pro názvy dokumentů v rámci logických kategorií včetně automatizovaného číslování nových dokumentů (např. žádosti o změny mohou mít „CRxxx_popis“, kde xxx je automaticky generované pořadové číslo).
- PK kontroluje a vynucuje jmenné konvence pro názvy dokumentů.
- PK umožňuje definovat skupiny uživatelů s možnostmi řízení uživatelského přístupu pro jednotlivé knihovny/složky/dokumenty s možností definice oprávnění typu: čtení/stažení dokumentu, rezervace dokumentu, vytvoření/vložení dokumentu, editace dokumentu, zneplatnění dokumentu.
- PK umožňuje kompletní export obsahu filesystému se zachováním rozdělení podle logických kategorií a všech verzí dokumentů pro offline procházení.

2.3 Projektové šablony

Dokumentace projektu bude standardizována prostřednictvím šablon ve formátu Office Open XML ve verzi pro Microsoft Office 2016, které budou uložené v PK.

Za vypracování šablon dokumentace odpovídá Vedoucí projektu Dodavatele a předkládá je ke schválení Vedoucímu projektu Zadavatele.

V dokumentech/šablonách se budou povinně vyplňovat minimálně následující metadata:

- Název (název dokumentu, není to název souboru)
- Předmět (stručný popis)
- Autor (hlavní autor dokumentu/garant)
- Společnost autora (ČÚZK, …)
- Klíč. slova (klíčová slova pro vyhledávání)

3. Definice jmenných konvencí názvů dokumentů

Všechny dokumenty ukládané na PK se musí řídit stanovenou jmennou konvencí.

Dokumentům uloženým v PK jsou přiřazena v MS SHP tzv. metadata. V rámci metadat je uvedena také historie verzí. Verze dokumentu uloženého v PK tedy není součástí názvu dokumentu, ale součástí metadat dokumentu v PK (resp. SP).

3.1 Proměnné masek výsledného názvu dokumentu

- <typ dokumentu> zkratka typu dokumentu – popis typu dokumentu, viz čl. 3.3.
- <verze aplikace> verze aplikace, ke které se dokument vztahuje. Používá se v případech, kdy je jednoznačný vztah dané dokumentace (release notes, protokol testování apod.) k dané verzi aplikace
- <pořadové číslo> jednoznačně generované číslo pro daný typ dokumentu
- <název> název dokumentu, charakterizující jeho obsah
- <datum> datum podle masky RRRRMMDD. Používá se pouze u typu dokumentu RV, VV a ZA, kde odpovídá datu konání jednání
- <přípona> přípona dokumentu (dle typu dokumentu, resp. zdrojové aplikace, kterou byl dokument vytvořen ze skupiny aplikací MS Office 2016)

Všechny uvedené proměnné jsou povinné, pokud jsou součástí masky daného typu dokumentu. Za formálně správné označení dokumentu odpovídá autor dokumentu.

Verze dokumentu je automaticky generována systémovými prostředky MS SHP po vložení/editaci. Verzování umožňuje prostředky Microsoft Office porovnávat a generovat rozdílové dokumenty.

3.2 Formáty výsledných názvů dokumentů definované maskami

3.2.1 Zápis z jednání (typ dokumentu=VV/RV/ZA)

- maska:
  <typ dokumentu><pořadové číslo>_<název>_<datum>.<přípona>
- příklad:
  RV001_Jednání ŘV_20221015.docx

3.2.2 Dokumentace vztahující se jednoznačně k dané verzi IDM

- maska:
  <typ dokumentu>_<verze_aplikace>.<přípona>
- příklad:
  RELN_3.3.0.03.docx

3.2.3 Dokumenty s jednoznačným názvem (TP, UP apod.)

Jde o dokumenty, kde je prefix doplněn názvem a přitom dokumenty nejsou číslované. Z důvodu kontroly na název dokumentu při vložení do PK je nutná rezervace s tímto názvem.

- maska:
  <typ dokumentu>_<název>.<přípona>
- příklad:
  TP_DF.docx

3.2.4 Ostatní dokumenty

- maska:
  <typ dokumentu><pořadové číslo>_<název>.<přípona>
- příklad:
  CR003_Změny v aplikaci.docx

3.2.5 Témata a zápisy z jednání

Pro dokumenty typu zápis vznikne pouze jeden dokument, který bude před vlastním jednáním obsahovat agendu a následně po schválení bude sloužit pro vlastní zápis z jednání. Samotný zápis z jednání bude v textu vhodným dohodnutým způsobem odlišen.

3.3 Typy dokumentů

Prefix	Typ dokumentů
AP	Akceptační protokoly
BR	Bezpečnost Resortu
BZ	Bezpečnostní dokumentace
CR	Analýzy
DE	Design dokument
HMG	Plánování
ME	Metodické pokyny, postupy, standardy
OS	Ostatní dokumenty
PIT	Protokol interního testování
PP	Předávací protokoly
RELN	Release notes
Sablona	Šablony
TI	Technická dokumentace
TP	Technologické postupy aplikace
TS	Testovací scénáře
UD	Uživatelská dokumentace
UP	Uživatelská příručka
UP_WS	Uživatelská příručka (část WS)
RV	Zápis Řídícího výboru
VN	Volný název
VV	Zápis Výkonného výboru
VY	Dokument výjimek
ZA	Zápisy ostatních schůzek
ZB	Zápis schůzky bezpečnosti
ZV	Zpráva o vývoji/Status report

4. Struktura PK

PK obsahuje knihovny a v rámci jednotlivých knihoven je možné vytvářet složky, které dále upřesňují typ dokumentu. Tyto složky je účelné vytvářet maximálně do 4. úrovně.

Složky musí mít následující jmennou konvenci:

„<číslo(a) pro řazení nadřízené složky/knihovny>-<číslo pro řazení aktuální složky> <název složky>“

Číslo pro řazení aktuální složky je jedinečné dvoumístné číslo ve formátu XX v rámci složky.

Detailní struktura PK ve smyslu složek a jejich struktury se může se v průběhu projektu vyvíjet. Neformální změny však podléhají odsouhlasení obou stran.

4.1 Výchozí struktura dokumentů PK

Struktura PK je navržena tak, aby první úroveň určovala pravidla pro dokumenty v knihovně umístěné, včetně workflow pro kontrolu a práv uživatelů. Dokumenty a složky v ní umístěné tedy budou dědit nastavení. Jednotlivé role a přístupová práva jsou popsány v kapitole 5.

Struktura PK:

- 00 Řízení PK
- 10 Bezpečnostní dokumentace (BZ)
- 20 Akceptační protokoly (AP)
- 30 Předávací protokoly (PP)
- 40 Dokumenty, výstupy
- 50 Zápisy Řídícího výboru (RV/ZV)
- 60 Provozní údržba - reporty
- 70 Dokumentace

4.2 Výchozí struktura dokumentů PK

Struktura PK je navržena tak, aby první úroveň určovala pravidla pro dokumenty v knihovně umístěné, včetně workflow pro kontrolu a práv uživatelů. Dokumenty a složky v ní umístěné tedy budou dědit nastavení. Struktura PK, jednotlivé role a přístupová práva jsou popsány v kapitole 5.

5. Skupiny a přístupová práva

PK obsahuje bezpečnostní skupiny, do kterých budou přiřazováni uživatelé po žádosti a schválení. Pro každou skupinu je definován přístup ke knihovnám a ke knihovnám a úroveň oprávnění, viz tabulka v kap. 5.1.

Žádost o přístup včetně cílové skupiny podává člen projektu prostřednictvím vedení projektu dané strany. Po potvrzení druhou stranou žádost realizuje administrátor PK.

5.1 Vazba mezi Knihovnami, skupinami a úrovní oprávnění

Jsou použity následující úrovně oprávnění:

- oprávnění čtení („**Čtení**“ jako čtenář) – opravňuje zejména k prohlížení, čtení, stahování,
- oprávnění úpravy („**Edit**“ jako editor) – nad rámec oprávnění čtení umožňuje rezervaci dokumentů, editace a vracení upravených verzí zpět,
- oprávnění návrh („**Schval**“ jako schvalovatel) – nad rámec oprávnění úpravy umožňuje především schvalování dokumentů do major verze rušení cizích rezervací,
- oprávnění úplné řízení („**Adm**“ jako administrátor).

	Skupina												
Knihovna	Administrace	Bezpečnost ČÚZK (schvalovatelé)	Bezpečnost ČÚZK (členové)	Bezpečnost ČÚZK (hosté)	Bezpečnost dodavatel	Vedení ČÚZK	Vedení dodavatel	Schvalovatelé ČÚZK	Členové ČÚZK	Schvalovatelé dodavatel	Členové dodavatel	Hosté ČÚZK	Hosté dodavatel
00 Řízení PK	Adm												
10 Bezpečnostní dokumentace (BZ)	Adm	Schval	Edit	Čtení	Edit								
20 Akceptační protokoly (AP)	Adm					Schval	Edit	Čtení	Čtení				
30 Předávací protokoly (PP)	Adm					Schval	Edit	Čtení	Čtení				
40 Dokumenty, výstupy	Adm					Schval	Edit	Schval	Edit	Schval	Edit	Čtení	Čtení
50 Zápisy Řídícího výboru (RV/ZV)	Adm					Schval	Edit						
60 Provozní údržba	Adm					Schval	Edit	Schval	Edit	Schval	Edit		
70 Dokumentace	Adm					Schval	Edit	Schval	Edit	Schval	Edit		

Příloha S03 - Práva a povinnosti manažera kybernetické bezpečnosti IS KII/VIS

Manažer kybernetické bezpečnosti IS KII/VIS odpovídá za systém řízení bezpečnosti informací pro daný IS KII/VIS a odpovídá se manažeru kybernetické bezpečnosti. Jeho povinností je:

- znalost ZKB, jeho prováděcích vyhlášek a souvisejících předpisů,
- zajistit bezpečnost primárních aktiv v rámci daného IS KII nebo VIS, tj. jejich důvěrnosti, dostupnosti a integrity,
- neprodleně hlásit kybernetické bezpečnostní incidenty IS KII/VIS manažerovi kybernetické bezpečnosti a vést jejich evidenci,
- připravovat pro manažera kybernetické bezpečnosti podklady pro NÚKIB,
- připravovat za IS KII/VIS pro manažera kybernetické bezpečnosti podklady pro jednání VŘKB,
- spolupracovat na 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, prošetřovat a určovat jeho příčiny a dokumentovat zvládání kybernetických bezpečnostních incidentů,
- vyhodnocovat účinnost preventivních a reaktivních opatření aplikovaných proti KBI,
- navrhovat úpravy bezpečnostní dokumentace společné pro všechny IS KII/VIS na základě zjištění z auditů kybernetické bezpečnosti, z výsledků vyhodnocení účinnosti systému řízení bezpečnosti informací a v souvislosti s prováděnými nebo plánovanými změnami v IS KII/VIS,
- zajišťovat testování zálohování a obnovy IS KII/VIS,
- na základě provedení analýzy rizik a hodnocení aktiv provádět aktualizaci dokumentu *Zpráva o hodnocení aktiv a rizik, Plán zvládání rizik*,
- zpracovávat ve spolupráci s architektem kybernetické bezpečnosti IS KII/VIS a garantem aktiv IS KII/VIS dokument *Prohlášení o aplikovatelnosti*,
- připravovat podklady do dokumentu *Zpráva z přezkoumání systému řízení bezpečnosti informací* a předkládat je manažerovi kybernetické bezpečnosti,
- garantovat implementaci schválených bezpečnostních opatření,
- do měsíce od informování manažerem kybernetické bezpečnosti zohledňovat reaktivní a ochranná opatření vydaná NBÚ v dokumentu *Zpráva o hodnocení aktiv a rizik*,
- doplnit dokument *Plán zvládání rizik* v případě, že hodnocení rizik aktualizované o nové zranitelnosti spojené s realizací reaktivního nebo ochranného opatření překročí stanovená kritéria pro přijatelnost rizik, a splnění této povinnosti oznámit manažerovi kybernetické bezpečnosti,
- spolupracovat při stanovování provozních pravidel a postupů k zajištění bezpečného provozu IS KII/VIS a navrhovat úpravy dokumentu *Politika řízení provozu a komunikací*,
- stanovovat bezpečnostní požadavky na změny IS KII/VIS spojené s jeho akvizicí, vývojem a údržbou a uplatňovat jejich zahrnutí do projektu, jehož součástí je akvizice, vývoj a údržba daného IS KII/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 osobami zastávajícími ostatní bezpečnostní role daného IS KII/VIS za účelem zajištění kybernetické bezpečnosti,
- odpovídat za to, že Dodavatel provede bezpečnostní testy zranitelnosti aplikací, pokud je provádění bezpečnostních testů začleněno ve smlouvě s Dodavatelem.

Práva manažera kybernetické bezpečnosti IS KII/VIS jsou:

- řídit a spolupracovat s architektem kybernetické bezpečnosti IS KII/VIS, garantem aktiv IS KII/VIS a administrátory technických aktiv pro zajištění splnění požadavků ZKB a VKB; k tomu vyžadovat součinnost a plnění úkolů,
- vyžadovat spolupráci a konzultaci s manažerem kybernetické bezpečnosti,
- posuzovat opodstatněné žádosti i výjimku v případech, kdy nelze pravidla, postupy a opatření stanovená v bezpečnostních dokumentech nebo vyžadovaná ZKB a VKB naplnit.

Způsob proaktivního zajištění bezpečnosti DMS

Základní roli v řízení bezpečnosti DMS bude mít Specialista bezpečnosti Dodavatele, který bude v souladu s požadavky ZD zastávat funkce Manažer kybernetické bezpečnosti VIS DMS a Architekt kybernetické bezpečnosti VIS.

Specialista bezpečnosti Dodavatele na začátku projektu převezme stávající. Z bezpečnostní dokumentace, která bude pravidelně aktualizována, budou vycházet jednotlivé vykonávané aktivity. Tyto aktivity budou plánovány a koordinovány na jednáních Bezpečnostního výboru, které se budou konat 1x za 6 týdnů. Z jednání bude standardně pořizován zápis a ukládán v úložišti projektové dokumentace.

Výčet aktivit bude samozřejmě plně v souladu s požadavky Zadávací dokumentace. V rámci zajištění proaktivního zajištění bezpečnosti bychom rádi zdůraznili dále uvedené skutečnosti.

Bezpečnostní testy:

Specialista bezpečnosti sleduje obsah připravované distribuce, na jehož základě navrhuje rozsah a zaměření prováděných bezpečnostních testů.

Bezpečnostní testy budou sestávat z několika fází:

Automatický bezpečnostní test – Dodavatel standardně využívá nástroje pro automatické skenování bezpečnostních slabin aplikace. Běžně používáme nástroje OWASp ZAP, SQLMap, NMap a další. Automatickým bezpečnostním testem je zkontrolována největší část aplikace.

Bezpečnostní test provedený bezpečnostním odborníkem – všechny části systému budou ohodnoceny z pohledu bezpečnostních rizik a zranitelností. V průběhu realizace změn systému bude k tomuto hodnocení přihlíženo – části sytému, které byly předmětem změny a které jsou z pohledu bezpečnosti více zranitelné, budou podrobeny penetračnímu testu prováděnému odborným pracovníkem Dodavatele.

Výše uvedené bezpečnostní testy jsou prováděny v rámci přípravy distribuce na prostředí Dodavatele. Kromě těchto testů bude Dodavatel provádět minimálně 1x ročně penetrační testy na ostrém prostředí. Pro test v prostředí Zadavatele je vždy připraven dokument Plán bezpečnostního testu.

Součástí bezpečnostních testů aplikace bude kontrola a zhodnocení použitých technologií z pohledu bezpečnosti.

Výstupem bezpečnostního testu bude protokol s popisem prováděného testu, dokumentací nálezů testu, ohodnocení jejich závažnosti a návrhem opatření.

Zajištění bezpečnosti v rámci vývoje nové verze systému:

Vývoj systému probíhá podle osvědčené metodiky Dodavatele. Metodika kromě aspektů zajištění kvality při dodržení nákladů řeší také bezpečnostní aspekty vyráběného produktu.

Bezpečnostní hlediska jsou součástí všech fází výroby. Zjednodušeně lze shrnout:

Zajištění bezpečnosti za základní součástí architektury aplikace. Musí být zohledněno při všech změnách architektury.

Vytvořený programový kód je podroben automatické statické analýze a code review, prováděnému seniorními SW inženýry. Součástí analýzy a review je hodnocení bezpečnosti

Testovací tým připravuje testovací scénáře pro ověření změn. Součástí těchto testů jsou vždy testy zabezpečení příslušné části aplikace

Sledování bezpečnostních zranitelností:

Dodavatel pravidelně sleduje novinky a upozornění v oblasti bezpečnosti. Sleduje informace vydávané NÚKIB a dodavateli SW. Mimo to sleduje nová doporučení OWASp a další zdroje. Na základě zjištěných informací informuje projektové týmy, které následně tyto informace aplikují na konkrétní systém. Tím se rozumí, že:

Vyhodnotí dopad informace na daný systém

Navrhnou opatření, které komunikují se zákazníkem

Na základě dohody se zákazníkem opatření zavádějí.

Správa logů aplikace:

Dodavatel má zkušenosti s monitoringem aplikací. Kromě běžných mechanismů logování událostí do souborů a jejich správy používá sofistikovaná řešení sběru logů do monitorovacích nástrojů a jejich následné vyhodnocení. Takto je možné průběžně sledovat stav systému, graficky znázornit trendy zatížení apod.

Bezpečnostní dokumentace:

Dodavatel se zavazuje spravovat bezpečnostní dokumentaci v souladu s požadavky zadávací dokumentace. Se správou dokumentace má zkušenosti z jiných projektů. Dodavatel je držitelem certifikátu ISO 27001.

Bezpečnost předávání informací mezi Zadavatelem a Dodavatelem:

Veškerý přístup do projektové kanceláře je řízen přístupovými oprávněními a pravidly projektového úložiště. Komunikace s úložištěm je šifrovaná protokoly, které vyhovují doporučením NÚKIB na šifrování komunikací.

Příloha S04 - Pravidla a způsob provádění bezpečnostních testů

1. Pravidla a způsob provádění bezpečnostních testů

1.1 Kritéria pro stanovení rozsahu bezpečnostního testování

Bezpečnostní testování je prováděno jako součást pravidelných testů nebo jako součást procesu řízení změn. Provádí se v odpovídajícím prostředí dle zaměření testu (produkční, testovací) a ve stanoveném rozsahu. Základním kritériem pro stanovení rozsahu bezpečnostního testování jsou:

- architektura testovaného IS,
- topologie sítě,
- v případě testování v rámci procesu řízení změn povaha změny IS.

V rámci návrhu rozsahu, zaměření a vhodného načasování bezpečnostního testu je posuzováno:

a) výskyt zranitelností jednotlivých komponent IS nebo prvků síťové infrastruktury;

b) typ komponent a jejich funkce (db server, file server);

c) umístění prvků v topologii sítě (interní síť, DMZ);

d) rozsah služeb poskytovaný IS a cílové uživatelské skupiny (pracovníci resortu, partneři, autorizovaní klienti, uživatelé v síti Internet);

e) zda změna IS zasahuje přímo do bezpečnostních vlastností IS např. webové aplikace (tedy je s přímým bezpečnostním dopadem, např. změna způsobu autentizace uživatele, změna zabezpečení dat v databázi), nebo změna má nebo může mít nepřímý bezpečnostní dopad nebo zasáhnout do bezpečnostních opatření IS (zavedená nová webová služba, doplněný modul bez přímé vazby na bezpečnostní opatření apod.);

f) rozsah změn.

Závazný minimální rozsah bezpečnostních testů v závislosti na charakteru změny vyjádřeném číslem verze je uveden v následující tabulce:

Iniciátor testu	**Rozsah prováděných bezpečnostních testů**
Pravidelný test	Provádí se plný rozsah bezpečnostních testů pokrývající všechny známé zranitelnosti a slabiny testovaných prvků na vybraném typickém prvku/prvcích.
Významná změna	Provádí se plný rozsah bezpečnostních testů pokrývající všechny známé zranitelnosti a slabiny testovaných prvků na všech prvcích dotčených změnou.
Malá změna	V případě, že v rámci změny bude implementována alespoň jedna změna IS s přímým nebo i nepřímým bezpečnostním dopadem, provádí se omezený rozsah bezpečnostních testů pokrývající všechny známé zranitelnosti a slabiny testovaných prvků souvisejících se změnou na všech prvcích dotčených změnou. V jiných případech se bezpečnostní testy neprovádí
Patch/hotfix	Provádí se omezený rozsah bezpečnostních testů minimálně pokrývající všechny známé zranitelnosti a slabiny veškerých aktualizovaných SW, aplikačních nebo systémových komponent.

Iniciátor testu	Rozsah prováděných bezpečnostních testů
	Bezpečnostní testy jsou prováděny na vybraném typickém prvku/prvcích dotčených změnou.
Bezpečnostní záplata nebo workaround	Provádí se volitelně specifické bezpečnostní testy k ověření eliminace všech zranitelností a slabin řešených danou bezpečnostní záplatou nebo workaroundem na vybraném typickém prvku/prvcích.
Výskyt nové zranitelnosti	Provádí se volitelně specifické bezpečnostní testy pokrývající všechny nové zranitelnosti a slabiny na vybraném typickém prvku/prvcích, v případě, že je vhodné ověřit možné působení a dopad nové zranitelnosti na IS.

Tab. 1: Minimální rozsah bezpečnostních testů dle změn

Výjimky z rozsahu bezpečnostních testů jsou možné pouze na základě souhlasu garanta aktiv IS.

Garant aktiv IS, bez ohledu na změny IS, provádí minimálně 1x ročně plný rozsah bezpečnostních testů.

1.2 Členění zranitelností podle závažnosti

CRITICAL

Kritická, vyžaduje zpravidla okamžitý zásah nebo odstavení systému.

IMPORTANT

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

MEDIUM

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

LOW

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

INFORMATION

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

1.3 Harmonogram a plán bezpečnostních testů

Součástí přípravy bezpečnostních testů v prostředí ČÚZK je harmonogram a plán testů.

Harmonogram i plán bezpečnostních testů navrhuje osoba, která bude realizovat testy vždy ve spolupráci se zástupci provozu ICT testem dotčených prvků a schvaluje jej Garant aktiva.

Minimální obsah harmonogramu bezpečnostních testů:

- datum, popřípadě období realizace bezpečnostních testů;
- časový rozsah realizace bezpečnostních testů;
- kontakty na osobu/osoby realizující bezpečnostní testy;
- kontaktní osoba/osoby na zástupce provozu ICT pro dotčené prvky.

Minimální obsah plánu bezpečnostních testů:

- jednoznačná identifikace všech testovaných prvků nebo síťového segmentu;
- identifikace prostředí ve kterém budou testy probíhat (produkční, testovací, vývojové);
- specifikace rozsahu testů pro jednotlivé typické prvky (testovací scénáře, metodika, nebo seznam testovaných zranitelností.

1.4 Pravidla provádění bezpečnostních testů

Testy musí být opakovatelné, aby prakticky prověřily webové aplikace, a musí být v produkčním prostředí prováděny neinvazivním způsobem, tj. bez zásahu do zdrojového kódu webové aplikace nebo jejich parametrů, které by mohlo zapříčinit narušení integrity, dostupnosti nebo důvěrnosti dat IS.

Pokud by hrozilo narušení integrity, dostupnosti nebo důvěrnosti dat IS, musí být testy prováděny na neprodukčním prostředí nebo tak, aby tato rizika byla eliminována (např. zálohou prostředí před testy, provádění testů v době ohlášené odstávky aplikace atd.).

Bezpečnostní testování je prováděno dle zpracovaných bezpečnostních testovacích scénářů. Po ukončení bezpečnostního testování je předložena garantovi aktiv IS Zpráva o výsledcích bezpečnostních testů.

1.5 Způsob provádění bezpečnostních testů

Před zahájením celkového testování je garantovi aktiv IS a manažerovi kybernetické bezpečnosti resortu předána informace o rozsahu bezpečnostních testů, včetně harmonogramu celkového testování s vyznačením termínů provádění bezpečnostních testů, a to v podobě dokumentu „Plán bezpečnostního testování“, Dokument „Plán bezpečnostního testování“ podléhá schválení ředitele odboru informatiky ČÚZK.

Bezpečnostní testy se provádí pouze na základě schváleného dokumentu „Plán bezpečnostního testování“. Dosažené výsledky jsou předkládány ve formě protokolu.

V případě zjištění kritické zranitelnosti v průběhu testování se zajistí odstranění chyby způsobující kritickou zranitelnost a provede opakování interních bezpečnostních testů se zaměřením na ověření odstranění kritické zranitelnosti.

Pro účely testování musí být předem zajištěn:

- testovací účet s přístupem do prostředí ČÚZK, v němž bude testována verze IS;
- přístup k webovým službám a aplikacím IS s právy

    - běžného externího uživatele;
    - uživatele oprávněného měnit údaje v IS;
    - správce;
- vzdálený přístup do interní sítě ČÚZK nebo fyzický přístup na pracoviště ČÚZK, pokud to bude pro testování potřebné;
- a možnost připojení koncového zařízení (testovacího notebooku nebo serveru) do testovacího prostředí ČÚZK.

Povinnosti související s prováděním bezpečnostních testů:

- bezpečnostní testy provádět dle schváleného dokumentu „Plán bezpečnostního testování“;
- při testování v produkčním prostředí brát ohled na dostupnost služeb poskytovaných testovanými prvky a dopad na jejich uživatele, důvěrnost a integritu dat v IS zpracovávaných (v případě narušení činnosti IS nebo ohrožení dat v IS zpracovávaných okamžitě přerušit testování a informovat garanta aktiva);
- v produkčním prostředí neověřovat prakticky zjištěnou zranitelnost vůči útoku „Denial of Services“ (DoS);
- 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 (nežádoucí nastavení oprávnění či zjištění jiné závažné slabiny umožňující únik, narušení integrity nebo ztrátu dostupnosti informací) okamžitě informovat garanta aktiv IS;
- v případě zjištění skutečností poukazujících na podezření ze zneužití pravomocí osob spravující nebo využívající IS (Insider) nebo v případě zjištění externího útočníka, tyto osoby nekontaktovat a informovat MKB.

Výsledky bezpečnostních testů jsou zpracovány do Zprávy o výsledcích bezpečnostních testů a předloženy s návrhy opatření a uvedením způsobu, jakým byly zjištěné kritické zranitelnosti vyřešeny.

V případě, že zpráva obsahuje zjištěné zranitelnosti, je nutné zajistit svolání schůzky za účelem projednání zjištění a návrzích řešení. Na schůzce se rozhodne o způsobu odstranění zranitelností nebo jejich eliminaci a dalším postupu. Toto je zaznamenáno do zápisu ze schůzky, který potvrzuje garant aktiv IS.

1.5.1 Typy realizací bezpečnostních testů

Bezpečnostní testy budou realizovány jako:

- automatizované testy - automatizovaným programovým vybavením,
- testy s manuálním podílem - automatizovaným programovým vybavením s podílem manuálního testováním
- manuální testy – manuálním ověřováním.

1.5.1.1 Automatizované testy a automatizované testy s manuálním podílem

Pro automatizované testování, resp. automatizované bezpečnostní testy s manuálním podílem bude použit některý z komerčních nástrojů. Druh aktuálně použitého nástroje bude uveden v dokumentu „Plán bezpečnostního testování“.

Automatizované bezpečnostní testy spolu s automatizovanými testy s podílem manuálního testování pomocí uvedeného nástroje ověří, zda webová aplikace, resp. webová služba,

neobsahuje některou ze známých zranitelností uvedených v Příloze 1, bodu 1. tohoto dokumentu, spadajících pod OWASP TOP 10.

(https://www.owasp.org).

1.5.1.2 Manuální testování

Při bezpečnostních testech realizovaných manuálně, je provedeno bezpečnostní testování prostřednictvím testů majících za cíl ověřit některé bezpečnostní vlastnosti, které není možné otestovat automatizovaným způsobem nebo by jejich automatizované testování nebylo dostatečně efektivní.

1.5.2 Specifické testy

Metodika OWASP obsahuje standardizované testy, tj. nezahrnuje všechny testovací scénáře zranitelností, které se mohou při vývoji nebo provozu informačního systému vyskytnout. Vzhledem k tomu jsou dále pro zajištění bezpečného fungování IS prováděny též i další specifické testy.

Specifické testy vycházejí a zohledňují možná specifika kódu, aktuální zranitelnosti a další specifika vyplývající z implementace nebo provozu IS v prostředí organizace, bezpečnostní události nebo incidenty, které se vyskytli u testovaných IS.

Za specifické testy jsou rovněž považovány testy ověření účinnosti bezpečnostních opatření aplikovaných k eliminaci již zjištěných zranitelností a slabin IS.

Seznam specifických zranitelností, které budou testovány, je uveden v Plánu bezpečnostního testování vč. testovacích scénářů.

1.5.2.1 Specifika testování webových aplikací a služeb

V rámci bezpečnostních testů jsou testovány externě přístupné části IS (webové aplikace a služby), 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 vždy obsahovat otestování:

a) ošetření všech uživatelských vstupů, (automatizované testy),
b) odolnosti proti známým typům útoků (SQL Injection, XSS, CSRF, Session Steal, ClickJacking apod.), (automatizované testy),
c) zákazu používaní tzv. skrytých polí pro důvěrná (citlivá) data, (testy s manuálním podílem),
d) zákazu používání přídavných identifikací uživatelských „session“ a obdobných autentizačních prostředků zakomponovaných v URL, (automatizované testy),
e) zákazu uvádění názvů souborů a adresářových cest v chybových hlášeních, (testy s manuálním podílem),
f) možností uživatelova odhlášení a automatického odhlášení po definované době jeho nečinnosti, (manuální testy),
g) omezení pro používání Cookies pouze na Cookies s časově omezenou platností, (testy s manuálním podílem),
h) Java applety a případné jiné komponenty musí být podepsány důvěryhodnou certifikační autoritou, (manuální testy),
i) komunikace aplikace s datovými zdroji v interní síti musí být autentizovaná, (manuální testy),
j) možnost napadení DoS útokem, (automatizované testy).

1.6 Ochrana dat v průběhu testování

V průběhu realizace bezpečnostních testů je zajištěna důvěrnost používaných dat, zejména pak:

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

2. Předmět bezpečnostních testů IS

Předmětem bezpečnostních testů IS jsou:

- operační systém IS;
- aplikace (např.: Dálkový přístup, ČÚZK Login, Platební portál, Služba sledování změn);
- webové služby;
- vč. všech externích částí IS (i nových).

3. Testovací scénáře

Testovací scénáře zahrnují následující údaje:

- název testovacího scénáře;
- ID testovacího scénáře;
- verze systému;
- 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.

Testovací scénáře pro automatizované, resp. automatizované testy s podílem manuálního testování, jsou konfigurovány v rámci použitého nástroje.

4. Zpráva o výsledcích bezpečnostních testů

O provedení bezpečnostních testů je pořizován dokument „Zpráva o výsledku bezpečnostních testů“ (dále jen „Zpráva“). Zpráva musí vždy obsahovat minimálně:

- datum a čas provedení bezpečnostního testu;
- na jakém prostředí bylo testováno;
- změny IS, které jsou dodávány a jaké změny 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;

- 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.

Zpráva se předkládá garantovi aktiv IS nejpozději do 2 týdnů od ukončení bezpečnostních testů vč. vyjádření k nalezeným zranitelnostem, která budou přenesena do *Registru zranitelností evidence testů"*.

Kritické zranitelnosti jsou oznamovány garantovi aktiv IS neprodleně po jejich AF zjištění.

Příloha S05 - Pravidla pro Dodavatele - minimální bezpečnostní standard pro významné dodavatele

Zadavatel přijal minimální bezpečnostní standard pro Dodavatele dle požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) (dále jen „ZoKB“) a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „VoKB“).

1. Obecné požadavky na Dodavatele

1.1. Dodavatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 5 Vyhlášky o kybernetické bezpečnosti, které musí splnit Zadavatel. Dodavatel se zavazuje řídit rizika spojená s plněním Smlouvy. Dodavatel je povinen neprodleně informovat Zadavatele o výsledcích analýzy rizik a možných rizicích spojených s poskytováním služeb Zadavateli, výsledcích analýzy rizik a přijatých opatřeních. Dodavatel nesmí přijmout rizika spojená s poskytováním služeb Zadavateli bez písemného souhlasu Zadavatele.

1.2. Dodavatel se zavazuje určit osobu odpovědnou ze Smlouvy za plnění bezpečnostních požadavků, do 14 dnů od účinnosti Smlouvy, pokud tato osoba není již Smlouvou definovaná.

1.3. Dodavatel se zavazuje prokazatelně seznámit všechny osoby podílející se na plnění předmětu Smlouvy s bezpečnostními požadavky, a to nejpozději do 15 dnů od účinnosti Smlouvy, případně od jejich zapojení se do plnění. O seznámení budou vedeny písemné záznamy.

1.4. Dodavatel se zavazuje vést provozní deník, kde budou zaznamenány všechny podstatné okolnosti vzniklé v souvislosti s plněním Smlouvy.

1.5. Dodavatel je povinen vést písemnou evidenci aktiv, které využívá k plnění Smlouvy (aktivem jsou např. data, informace, SW, HW, lidské zdroje, prostory, licence, Poddodavatel), tuto evidenci zpřístupní na vyžádání Zadavatele.

1.6. Dodavatel se zavazuje řídit přístupy a oprávnění osob podílejících se na plnění předmětu Smlouvy tak, aby minimalizoval neoprávněný přístup k aktivům Zadavatele.

1.7. Dodavatel je povinen vést systémovou a provozně technickou bezpečnostní dokumentaci.

1.8. Dodavatel je povinen dodržovat platné smluvní podmínky výrobců HW a SW používaného k plnění předmětu Smlouvy a dodržovat licenční čistotu dle zákona č. 121/2000 Sb., o autorském právu.

1.9. Dodavatel se zavazuje neprodleně informovat Zadavatele o kybernetických bezpečnostních incidentech (viz § 7 ZoKB) a poskytovat nezbytnou součinnost při plnění požadavků specifikovaných v § 8 ZoKB. Dodavatel se dále zavazuje poskytnout nezbytnou součinnost potřebnou pro vyšetření a případné vyřešení daného kybernetického bezpečnostního incidentu.

1.10. Dodavatel bere na vědomí, že po celou dobu Smlouvy je povinen poskytnout Zadavateli nezbytnou součinnost pro ověření, zda Dodavatel splňuje požadavky ZoKB.

2. Poddodavatelé a ovládání

2.1. Pro realizaci předmětu plnění má Dodavatel právo použít smluvní Poddodavatele. Seznam Poddodavatelů předložil Dodavatel před podpisem Smlouvy. Dodavatel má právo použít k plnění i další Poddodavatele po předchozím odsouhlasení Zadavatelem. Zadavatel odsouhlasení nového Poddodavatele bezdůvodně neodmítne. V případě, že Dodavatel využívá Poddodavatele k výkonu činností

vymezených ve smlouvě, odpovídá za kvalitu, bezpečnost a včasnost plnění stejným způsobem, jako by činnost prováděl sám.

2.2. V případě, že Dodavatel využívá Poddodavatele k výkonu činností definovaných smlouvou, je povinen informovat Poddodavatele o požadavcích na bezpečnost informací a bezpečnostních pravidlech, které je povinen dodržovat při výkonu dané činnosti alespoň ve stejném rozsahu, v jakém to od Dodavatele Zadavatel požaduje.

2.3. Dodavatel je povinen Zadavatele předem informovat o významné změně ovládání Dodavatele. Ovládáním se zde rozumí zejména ovládání či řízení podle § 74 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, či ekvivalentní postavení. Notifikační povinnost může být taktéž navázána na změnu skutečného majitele v evidenci skutečných majitelů (§ 118b a násl. zákona č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob a o evidenci svěřeneckých fondů). Zadavatel je oprávněn odstoupit od Smlouvy v případě významné změny kontroly Dodavatele s tím, že změnou kontroly Dodavatele se rozumí změna ovládání či řízení podle § 74 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, změna vlastnictví zásadních aktiv, popřípadě změna oprávnění nakládat s těmito aktivy, využívanými Dodavatelem k plnění Smlouvy.

3. Bezpečnost informací a ochrana osobních údajů

3.1. Dodavatel deklaruje, že má pro plnění předmětu Smlouvy plně nastavené a využívané procesy k zajištění bezpečnosti informací v souladu s ISO/EC 27001.

3.2. Dodavatel se zavazuje pro případ, že se v průběhu plnění předmětu Smlouvy dostane do kontaktu s osobními údaji, že je bude ochraňovat a nakládat s nimi plně v souladu s příslušnými právními předpisy, tj. zejména se zákonem č. 110/2019 Sb., o zpracování osobních údajů, a Obecným nařízením o ochraně osobních údajů (GDPR - Nařízení Evropského parlamentu a Rady (EU) 2016/679), tak, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich zneužití, změně, zničení či ztrátě, a to i po ukončení plnění Smlouvy. 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.

3.3. Smluvní strany se v případě, že se Dodavatel dostane do pozice zpracovatele osobních údajů ve správě Zadavatele, ve smyslu příslušných ustanovení zákona o ochraně osobních údajů, zavazují uzavřít dodatek ke Smlouvě spočívající v dohodě o zpracování osobních údajů, pokud platná Smlouva toto již nezahrnuje.

3.4. Dodavatel je povinen zajistit, aby do informačních systémů Zadavatele obsahující informace s osobními údaji měli přístup pouze osoby podílející se na plnění předmětu Smlouvy, které k tomu mají oprávnění, a to pouze k těm údajům a zdrojům, které jsou nezbytné pro plnění jejich povinností – tzv. princip need-to-know.

3.5. Zadavatel je povinen každé osobě podílející se na plnění předmětu Smlouvy na straně Dodavatele, která má přístup do informačních systémů s informacemi a osobními údaji Zadavatele prostřednictvím sítě internet, vydat osobní a jedinečný identifikační kód pro tyto účely - uživatelské ID. Uživatelské ID nesmí být nikdy ani v budoucnu postoupeno jiné osobě.

3.6. Dodavatel je povinen každé osobě podílející se na plnění předmětu Smlouvy na straně Dodavatele, která má přístup do informačních systémů s informacemi a osobními údaji Zadavatele, vydat osobní a jedinečný identifikační kód pro tyto účely - uživatelské ID. Uživatelské ID nesmí být nikdy ani v budoucnu postoupeno jiné osobě.

3.7. Dodavatel je povinen zajistit, aby každé osobě podílející se na plnění předmětu Smlouvy na straně Dodavatele bylo povoleno zpracovávat informace a Osobní údaje Zadavatele, pouze pokud jim jsou přiděleny ověřovací údaje (credentials), např. k úspěšnému provedení ověřovacího postupu týkajícího se buď specifické operace zpracování, nebo sady operací zpracování.

3.8. Zadavatel/Dodavatel je povinen deaktivovat ověřovací údaje, pokud je osoba podílející se na plnění předmětu Smlouvy na straně Dodavatele prohlášena nezpůsobilou nebo jí je odebráno oprávnění přístupu do informačních systémů Zadavatele nebo ke zpracování informací a osobních údajů Zadavatele.

3.9. Dodavatel je povinen zajistit, aby nosiče obsahující informace a Osobní údaje Objednavatele byly u Dodavatele k dispozici pouze pověřeným osobám podílejícím se na plnění předmětu Smlouvy na straně Dodavatele.

3.10. Dodavatel je povinen zajistit, aby informační systémy Zadavatele a hmotné nosiče, na kterých jsou uloženy informace a Osobní údaje Zadavatele, byly u Dodavatele uschovány v bezpečném prostředí znemožňující vyzrazení, modifikaci, zničení či jiné ovlivnění informací a osobních údajů Zadavatele.

3.11. Dodavatel je povinen zajistit, aby informace a Osobní údaje Zadavatele byly od Dodavatele distribuovány prostřednictvím veřejných elektronických komunikačních sítí pouze tehdy, pokud jsou zakódovány nebo jinak zašifrovány nebo je použit jiný mechanismus zajišťující, aby údaje nebyly srozumitelné nebo aby s nimi nemohly manipulovat třetí osoby.

3.12. Dodavatel je povinen zajistit, aby přístup do prostor u Dodavatele, kde jsou umístěny informační systémy a nosiče Zadavatele s uloženými informacemi a Osobními údaji Zadavatele, měli pouze osoby, které mají přidělena řádná oprávnění a které mají oprávněný důvod ke vstupu.

3.13. Dodavatel je povinen zajistit, aby osoby podílející se na plnění předmětu Smlouvy na straně Dodavatele byly vázány povinností mlčenlivosti o informacích, Osobních údajích Zadavatele a bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení informací a osobních údajů Zadavatele, přičemž tato povinnost trvá i po skončení zaměstnání nebo příslušných prací.

3.14. Dodavatel je povinen zajistit, aby při ukončení Smlouvy byly informace a Osobní údaje Zadavatele předány a následně smazány z nosičů, informačních systémů a dalších zařízení Dodavatele (včetně bezpečnostních záloh). O smazání bude předáno Objednavateli čestné prohlášení.

3.15. Osoby podílející se na plnění předmětu Smlouvy na straně Dodavatele jsou povinny zejména:

3.15.1. odpovídajícím způsobem chránit informace a Osobní údaje Zadavatele, a to zcela bez ohledu na jejich formu uložení (flash disky, mobilní telefony, papírové dokumenty, notebooky, disky, vyměnitelná média apod.),

3.15.2. obrátit se na Zadavatele s žádostí o pomoc, pokud by hrozilo, že jakýmkoli způsobem bude ohroženo plnění povinností dle tohoto Minimálního bezpečnostního standardu.

3.16. Osoby podílející se na plnění předmětu Smlouvy na straně Dodavatele se musí zdržet zejména:

3.16.1. předávání Osobních údajů a dalších chráněných informací Zadavatele jakýmkoli neoprávněným osobám,

3.16.2. předávání Osobních údajů Zadavatele prostřednictvím veřejně dostupných cloudových služeb.

3.17. Dodavatel nemá oprávnění k využití dat pro svou potřebu, např. statistické účely, evidenční podklady vyúčtování apod.

3.18. Dodavatel je povinen zajistit postup nahlašování bezpečnostních incidentů, reagování na ně a jejich vyřizování.

3.19. Dodavatel je povinen v rámci procesu pro šetření bezpečnostních incidentů zajistit, že Zadavatel bude bezodkladně informován o jakémkoli bezpečnostním incidentu, který má či může mít vliv na informace a Osobní údaje Zadavatele.
3.20. Dodavatel je povinen přijmout nezbytná opatření, aby zaměstnanci byli dobře obeznámeni s těmito minimálními bezpečnostními požadavky a s následky jakéhokoliv jejich porušení.
3.21. Minimální doba pro uchování všech údajů zaznamenaných dle výše uvedených ustanovení je 18 měsíců.

4. Řízení kontinuity činností a obnovy po havárii

4.1. Dodavatel je povinen ve spolupráci se Zadavatelem pracovat na přípravě plánů obnovy po havárii, případně poskytnout nezbytnou součinnost pro jejich přípravu.
4.2. Všechny připravené plány obnovy po havárii budou Zadavatelem v pravidelných intervalech testovány na svou účinnost a proveditelnost. Dodavatel je povinen se daného testování v nezbytné míře zúčastnit. O termínu testování bude Dodavatel v dostatečném předstihu informován Zadavatelem.
4.3. V případě zjištění nedostatků v testovaných plánech obnovy po havárii je Dodavatel povinen v patřičném rozsahu dané plány upravit dle výsledků testování tak, aby byly proveditelné a účinné.
4.4. V případě výskytu havárie Dodavatelem dodávaného systému je Dodavatel povinen účastnit se jeho obnovy v rozsahu stanoveném připravenými plány obnovy po havárii.

5. Audit kybernetické bezpečnosti

5.1. Zadavatel si vyhrazuje právo provádět u Dodavatele zákaznické audity zaměřené na plnění procesních, bezpečnostních a legislativních povinností při poskytování služeb Zadavateli nebo zpracování údajů Zadavatele. Dodavatel bere na vědomí, že po dobu trvání Smlouvy umožní Zadavateli zejména provést kontrolu souladu s požadavky ZoKB a souvisejících právních předpisů.
5.2. Zadavatel je povinen písemně sdělit Dodavateli termín, místo a nezbytný rozsah auditu nejpozději 14 dní před zahájením auditu.
5.3. Zadavatel je povinen písemně sdělit jména osob, která se budou auditu účastnit. Tyto osoby mohou zahrnovat i osoby třetích stran.
5.4. Zadavatel je povinen informovat o výsledcích auditu Dodavatele nejpozději do 30 dnů od jeho skončení.
5.5. Dodavatel je povinen poskytnout nezbytnou součinnost, předložit na vyžádání dokumenty a realizovat schválená nápravná opatření.

6. Technická opatření

Dodavatel se zavazuje po dobu trvání Smlouvy ve svém prostředí realizovat technická opatření a dodržovat následující požadavky:

6.1. Požadavky na zajištění fyzické bezpečnosti prostor Dodavatele dle § 17 VoKB k zajištění ochrany aktiv a zamezení neoprávněného vstupu, a to především
  6.1.1. definovat bezpečnostní zóny k zabezpečení v minimálním rozsahu (serverovna, uživatelské prostory, prostory dostupné pro třetí strany),
  6.1.2. definovat pro jednotlivé bezpečnostní zóny vhodná bezpečnostní opatření na zajištění proti neoprávněnému vstupu, přičemž zóna typu serverovna

musí mít automaticky řízený a evidovaný systém vstupů, musí být zajištěna proti vniknutí, a musí být chráněna před požárem a vysokou teplotou,

6.1.3. zajistit, aby všechny zóny byly náležitě monitorovány pro případnou detekci neoprávněného vstupu a předcházení poškození umístěného vybavení.

6.2. Požadavky na zajištění bezpečnosti komunikačních sítí dle § 18 VoKB, tj, segmentace sítě, zajištění důvěrnosti a integrity vzdáleného připojení, využití nástroje k zajištění integrity sítě, a to především

6.2.1. síť musí být rozdělena do několika logických síťových segmentů dle funkce či účelu (typicky uživatelský segment, IT segment, serverový segment, tiskový segment, DMZ apod.),

6.2.2. komunikace mezi jednotlivými segmenty musí být automaticky řízena a kontrolována na úrovni firewallu definujícího komunikační pravidla mezi segmenty,

6.2.3. v rámci sítě musí být aktivně blokovány potenciálně nebezpečné komunikační protokoly,

6.2.4. přístup k interní síti musí být kontrolován a povolen jen oprávněným uživatelům/zařízením,

6.2.5. při používání vzdáleného přístupu musí být takové vzdálené spojení šifrované za použití protokolů doporučených Národním úřadem pro kybernetickou a informační bezpečnost.

6.3. Požadavky správy a ověřování identit dle § 19 VoKB, a to především

6.3.1. identity všech uživatelů, administrátorů a aplikací musí být spravovány centrálním nástrojem,

6.3.2. před přihlášením uživatele musí dojít k ověření jeho identity,

6.3.3. po pěti neúspěšných pokusech o přihlášení uživatele musí dojít k zablokování jeho účtu alespoň na dobu 30 minut,

6.3.4. přihlašovací údaje musí být uloženy v šifrované formě a odolné proti odcizení, zneužití a případným útokům,

6.3.5. při nečinnosti uživatele po dobu delší než 15 minut musí dojít k odhlášení uživatele či uzamčení jeho sezení a uživatel musí být donucen znovu poskytnout své přihlašovací údaje,

6.3.6. pro přihlašování uživatelů musí být použita vícefaktorová autentizace,

6.3.7. není-li možné využít vícefaktorovou autentizaci, musí být používána autentizace pomocí kryptografických klíčů,

6.3.8. není-li možné využít autentizace pomocí kryptografických klíčů, musí být vynucena politika hesel

6.3.8.1. hesla uživatelů musejí mít minimální délku 12 znaků,

6.3.8.2. hesla administrátorů a technických či servisních účtů musejí mít minimální délku 17 znaků,

6.3.8.3. uživatelé musejí mít možnost použít hesla alespoň 64 znaků dlouhá,

6.3.8.4. heslo musí obsahovat alespoň jedno malé a jedno velké písmeno, číslici a speciální znak,

6.3.8.5. uživatelé si mohou změnit heslo nejdříve 24 hodin od poslední změny hesla,

6.3.8.6. nesmějí být používána nejčastěji používaná hesla, např. „heslo“, „123456“, „qwertz“ apod.

6.3.8.7. heslo nesmí obsahovat mnohokrát se opakující znaky, přihlašovací jméno, e-mail, název systému apod.,

6.3.8.8. uživatelé při změně hesla nesmějí použít žádné z předchozích 12 hesel,

6.3.8.9. po maximálně 18 měsících musí docházet k vynucené změně hesla,

6.3.8.10. při vytvoření úvodního hesla nebo hesla pro obnovení musí být toto heslo po jeho prvním použití ihned zneplatněno a uživatel musí být nucen zvolit si své vlastní,
6.3.8.11. uživatelé musejí být informování o politice hesel.

6.4. Požadavky na řízení přístupových oprávnění dle § 20 VoKB, a to především
6.4.1. pro přidělování uživatelských oprávnění je zaveden centrální systém,
6.4.2. oprávnění jsou přidělována na základě evidované žádosti, která je schválena oprávněnou osobou,
6.4.3. všechna přidělená oprávnění jsou pravidelně revidována (alespoň jednou ročně) a nepotřebná oprávnění jsou odebírána.

6.5. Požadavky na ochranu před škodlivým kódem dle § 21 VoKB, a to především
6.5.1. Dodavatel bude využívat nástroj na ochranu před škodlivým kódem instalovaný alespoň na koncových stanicích, serverech, datových úložištích, prvcích komunikační sítě a přiměřeně na mobilních zařízeních,
6.5.2. virové definice daného nástroje musejí být aktualizovány alespoň jednou za den,
6.5.3. při vydání nové verze nástroje musí být instalována aktualizace nejpozději do 3 měsíců od publikace,
6.5.4. musí být aktivně řízeno používání vyměnitelných médií – jejich použití musí být omezeno jen na vybrané pracovníky, kteří je nutně potřebují pro výkon své práce,
6.5.5. při používání vyměnitelných zařízení musí být jejich obsah oskenován nástrojem na ochranu před škodlivým kódem předtím, než k němu může přistoupit uživatel,
6.5.6. uživatelé nesmějí mít možnost spustit neautorizovaný software.

6.6. Požadavky na zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů v rozsahu § 22 VoKB, a to především
6.6.1. provozní a bezpečnostní události na aktivech souvisejících s poskytováním služby jsou zaznamenávány alespoň v rozsahu § 22 odst. 2 písm. d) VoKB,
6.6.2. zaznamenané události musí obsahovat alespoň informace uvedené v § 22 odst. 2 písm. b) VoKB,
6.6.3. zaznamenané události jsou uchovávány v centrálním úložišti po dobu alespoň 18 měsíců, kde musí být zajištěna jejich integrita,
6.6.4. napříč prostředím Dodavatele musí docházet k synchronizaci času s jednotným zdrojem času,
6.6.5. v případě kybernetických bezpečnostních událostí/incidentů bude možné předat příslušné logy Zadavateli.

6.7. Požadavky na detekce kybernetických událostí dle § 23 VoKB, a to především:
6.7.1. v prostředí sítě dojde k implementaci nástroje IPS umožňujícího identifikaci a případnou blokaci nežádoucí komunikace jak v rámci interní sítě, tak mezi dalšími sítěmi, např. internetem,
6.7.2. záznamy o takové komunikaci budou ukládány do centrálního úložiště logů.

6.8. Požadavky na sběr a vyhodnocování událostí dle § 24 VoKB, a to především
6.8.1. v rozsahu služeb poskytovaných Zadavateli nasadí Dodavatel nástroj pro sběr a vyhodnocování kybernetických bezpečnostních událostí,
6.8.2. vyhodnocování bude probíhat nad logy, které jsou ukládány v rámci centrálního úložiště,
6.8.3. informace o potenciálních kybernetických bezpečnostních incidentech bude předávána osobě s kompetencí kybernetické bezpečnosti k vyhodnocení,
6.8.4. informace z nástroje budou používány pro průběžné zlepšování zabezpečení prostředí Dodavatele v rozsahu poskytovaných služeb.

6.9. Požadavky na aplikační bezpečnost dle § 25 VoKB, a to především
6.9.1. poskytuje-li Dodavatel Zadavateli aplikaci či jiný informační systém, zajistí před jeho nasazením do provozu v prostředí Zadavatele penetrační test a

zajistí nápravu všech zjištěných zranitelností ohodnocených skórem CVSS v3 7.0 a vyšší, případně všechny vysoké a kritické zranitelnosti, není-li používáno skóre CVSS,

6.9.2. obdobně postupuje Dodavatel v případě, kdy připravuje významnou změnu daného systému.

6.10. Požadavky na kryptografické prostředky dle § 26 VoKB, a to především

6.10.1. využívá-li Dodavatel při poskytování služby Zadavateli kryptografických prostředků, musí být používány pouze takové kryptografické algoritmy, které doporučuje Národní úřad pro kybernetickou a informační bezpečnost,

6.10.2. využívá-li k tomuto účelu Dodavatel vlastních klíčů a certifikátů, zajistí zabezpečení životního cyklu těchto kryptografických prostředků.

6.11. Požadavky na zajištění úrovně dostupnosti informací dle § 27 VoKB, a to především v případě, kdy poskytuje Dodavatel informační systém jako službu, případně přímo zajišťuje jeho provoz a další rozvoj, zajistí ve spolupráci se Zadavatelem jeho dostupnost dle výsledků provedené analýzy dopadů na straně Zadavatele.

6.12. Požadavky na bezpečnost průmyslových, řídících a obdobných systémů dle § 28 VoKB, a to především poskytuje-li Dodavatel Zadavateli systémy spadající do kategorie průmyslové, řídicí a obdobné systémy, zajistí jejich kybernetickou bezpečnost specifickými opatřeními

6.12.1. systém bude provozován v komunikační síti oddělené od ostatní infrastruktury,

6.12.2. vzdálený přístup k takovému systému bude omezen pouze na specifické IP adresy po vyhrazené komunikační lince oddělené od běžného vzdáleného přístupu,

6.12.3. na úrovni komunikační sítě musí být aktivně blokována komunikace vedoucí na potenciálně zranitelná rozhraní daného systému,

6.12.4. v případě výpadku systému musí existovat detailní postup pro obnovu jeho chodu.

6.13. Dodavatel se zavazuje plnit požadavky na likvidaci médií dle přílohy 4 VoKB.

Příloha S06 – Průběžný rozvoj, bezpečnost a údržba DMS

1. Průběžný rozvoj, bezpečnost a údržba DMS

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

Zadavatel v této souvislosti požaduje, aby Dodavatel v předstihu před fakturací za průběžný rozvoj, bezpečnost a údržbu DMS předkládal Zadavateli k odsouhlasení výkazy a přehledy s výsledky činností za dané období. Odsouhlasené měsíční výkazy Zadavatelem jsou nedílnou součástí faktury za Průběžný rozvoj, bezpečnost a údržbu DMS. Kumulované nevyčerpané ČLD z předchozích měsíců, maximálně však celkem 10 ČLD za služby průběžného rozvoje DMS, 10 ČLD za služby průběžné údržby DMS a 2 ČLD za služby věnované bezpečnosti DMS, bude možné převádět do následujícího měsíce. Kumulaci nevyčerpaných ČLD je možné realizovat nejvýše v rámci jednoho čtvrtletí poskytování služby. Průběžný rozvoj, bezpečnost a údržba DMS budou Dodavatelem vykazovány Zadavateli 1x měsíčně ve výkazu práce, jehož vzor je uveden v Příloze ZD07. V případě dosažení 90% měsíčního paušálního plnění v každé vykazované části je Dodavatel povinen bezodkladně kontaktovat Zadavatele, který následně stanoví další postup (plnění v maximálním rozsahu, popřípadě objednání víceprací).

Do paušálního poplatku za průběžný rozvoj, bezpečnost a údržbu DMS Účastník zadávacího řízení zahrne kromě nákladů na výše uvedený počet ČLD na průběžný rozvoj a údržbu DMS zejména náklady na zajištění monitoringu provozu a dále všech podpůrných a souvisejících činností s plněním VZ jako jsou např. nepřímé náklady, administrace projektu (příprava zápisů, výkazů, akceptací, nabídek, komunikace se Zadavatelem, účast na projektových schůzkách (např. Řídící výbor – ŘV – 1x za 6 týdnů a Výkonný výbor VV – 1x za 14 dní, Bezpečnostní výbor – 1x za 6 týdnů, které se konají v budově Zadavatele).

Do paušálního poplatku za průběžný rozvoj, bezpečnost a údržbu DMS musí být započítány i náklady související se zajištěním produktů OB-TA, Long-Term Docs SDK a Versity ScoutAM po celou dobu účinnosti smlouvy, popřípadě i přechod na jinou technologii. Více informací je uvedeno v čl. **Chyba! Nenalezen zdroj odkazů.**ZD.

1.1 Průběžný rozvoj 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 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 aktuální verzi DB Oracle a aktuální verze systémů pro aplikační část před ukončením Smlouvy.

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.

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 VZ, nebo v části již modifikované v rámci plnění dle této VZ.

V rámci průběžné údržby budou vyřešeny opravy nesprávné funkčnosti DMS (např. rozdílné chování proti uživatelské příručce) v částech nemodifikovaných v rámci plnění dle této VZ (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.

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 VZ (dále jen „záruční závada“) budou provedeny zdarma v rámci záručního servisu.

1.2 Zajištění bezpečnosti DMS

Nedílnou součástí Průběžného rozvoje, bezpečnosti a údržba DMS je zajištění bezpečnosti DMS ČÚZK v souladu s VoKB a platnými vnitřními předpisy a aktualizace bezpečnostní dokumentace.

Při realizaci předmětu plnění musí Dodavatel garantovat zachování bezpečnosti DMS ČÚZK alespoň na stávající úrovni, pokud nějaký závazný právní předpis nebude požadovat úroveň vyšší. Dodavatel je podle VKB klasifikován jako významný, a proto musí splňovat požadavky bezpečnostního standardu uvedené v příloze S05 – Pravidla pro dodavatele – minimální bezpečnostní standard pro významného dodavatele. Při realizaci předmětu plnění musí Dodavatel minimálně zajistit splnění požadavků kladených na ISVS, KII a VIS dle platných právních předpisů.

Seznam bezpečnostních dokumentů Zadavatele pro DMS ČÚZK je strukturován podle požadavku VKB.

V rámci bezpečnosti DMS ČÚZK Zadavatel požaduje mimo jiné také zajištění:

1.2.1 Ochrany informací

Zadavatel požaduje všechny informace týkající se předmětu plnění (dále též jen „informace“)

klasifikovat a přidělovat jim následující stupně důvěrnosti:

- Veřejné – informace určené Garantem aktiva ke zveřejnění.
- Klasifikované – informace, jejichž zveřejnění mimo Zadavatele by mohlo narušit bezpečnost informací, jsou určeny pouze pro zaměstnance Zadavatele nebo Dodavatele.
  - Interní – informace jsou poskytovány na základě smlouvy nebo prohlášení o ochraně informací.
  - Diskrétní – informace jsou poskytovány pouze určenému okruhu osob, který je evidován.
  - Přísně diskrétní – informace jsou poskytovány pouze předem určeným osobám na základě předávacího protokolu.

Stupeň ochrany klasifikovaných informací bude označen na každém klasifikovaném dokumentu na stránce v pravém horním rohu. Dokumenty v klasifikaci Veřejné toto označení mít nemusí.

1.2.2 Činností Dodavatele/Specialisty kybernetické bezpečnosti

Zadavatel požaduje, aby specialista kybernetické bezpečnosti Dodavatele dle VoKB zastával pro DMS roli:

- manažer kybernetické bezpečnosti IS,

Popis uvedené role, včetně povinností, které z těchto rolí vyplývají, jsou uvedeny v příloze S03 - Práva a povinnosti manažera kybernetické bezpečnosti IS KII/VIS.

1.2.3 Činností v oblasti dokumentace

Dodavatel musí:

Do 6 měsíců od začátku účinnosti smlouvy a dále 1x ročně:

- dle ZoISVS vytvořit respektive aktualizovat a nadále udržovat aktuální provozní dokumentaci všech částí DMS ČÚZK,

- dle ZoKB a VoKB aktualizovat a nadále udržovat aktuální bezpečnostní dokumentaci o prováděných bezpečnostních opatřeních všech částí DMS ČÚZK.

Do konce smlouvy vytvořit dokumentaci v souladu s vyhláškou č. 360/2023 Sb.

1.2.4 Dalších činností

- sledovat zejména:
  - **a)** informační servis Národního úřadu pro kybernetickou a informační bezpečnost,
  - **b)** security bulletiny/advisory společností, jejichž SW se v DMS ČÚZK využívá,
  - **c)** další zdroje zabývající se zveřejňováním zranitelností, a pravidelně Zadavatele informovat o možných relevantních hrozbách a zranitelnostech souvisejících s DMS ČÚZK, navrhovat opatření na jejich eliminaci,
- navrhovat změny (zlepšení) v oblasti bezpečnosti DMS ČÚZK,
- z hlediska bezpečnosti průběžně sledovat a kontrolovat projednávané změny a úpravy DMS ČÚZK (analýzy a návrhy řešení) a navrhovat případné úpravy,
- pro oblasti zasažené/měněné v dodávce DMS ČÚZK provádět z hlediska bezpečnosti kontrolu architektury a kódu (code review),
- při každé změně DMS ČÚZK předat do měsíce aktualizaci havarijních plánů (tj. plánů obnovy) DMS ČÚZK včetně postupů při obnově provozu DMS ČÚZK,
- do jednoho měsíce od začátku účinnosti smlouvy vytvořit a udržovat aktuální dokument popisující způsob bezpečné elektronické komunikace zabraňující přístupu k informacím týkajících se předmětu plnění (dále též „informace“) neoprávněné osobě, a to jak při předávání a výměně informací nebo jejich ukládání (zpracování) v rámci týmu Dodavatele, tak mezi Dodavatelem a Zadavatelem, a tento způsob zajistit,

- trvale zajišťovat bezpečnost informací a bezpečnost činností při vlastním plnění Dodavatele (zabezpečení infrastruktury, postupů, ochrany dat apod.),
- svolávat minimálně 1x za 6 týdnů v sídle Zadavatele jednání k zajištění bezpečnosti DMS ČÚZK a pořizovat z nich zápisy. Na jednáních informovat o aktuálním stavu plnění činností, úkolů, konzultovat spolu se zástupcem Zadavatele problémy, předkládat návrhy na zlepšení bezpečnosti, předkládat k připomínkám návrhy/aktualizace dokumentů aj.,
- průběžně zajišťovat aktuálnost dokumentů týkajících se bezpečnosti uvedených v příloze ZD06 - Přehled bezpečnostní dokumentace Zadavatele pro DMS.

1.2.5 Činností v oblasti bezpečnostních testů

Zadavatel požaduje, aby Dodavatel prováděl bezpečnostní testy DMS ČÚZK v souladu s požadavky uvedenými v příloze S04 - Pravidla a způsob provádění bezpečnostních testů. Zjištěné zranitelnosti bezodkladně vyhodnotí a navrhne v součinnosti se Zadavatelem jejich minimalizaci. Na základě zjištěných zranitelností nebo při jiných bezpečnostních testech, auditech, penetračních testech, anebo na základě zjištění výskytu možné zranitelnosti musí Specialista kybernetické bezpečnosti zajistit včasný návrh a realizaci opatření schválených Zadavatelem. Zadavatel požaduje, aby k minimalizaci rizik spojených s možnými chybami při vývoji externích aplikací Dodavatel při vývoji používal nástroj pro kontrolu bezpečnosti např. Netsparker, Burp suite professional, Acunetix, Metasploit, Nessus[1] apod.

1.3 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 vlastními silami. Zadavatel umožní zasílání vybraných notifikačních zpráv z monitoringu Dodavateli.

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

[1] Zadavatel umožňuje ve smyslu § 89 ZZVZ nabídnout technicky rovnocenné řešení.

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-A
Aplikační test - kontrola počtu zpráv odeslaných do OB-A, jejichž přijetí v OB-A není potvrzené
Aplikační test běhu aplikace pro odesílání dokumentů z DMS do OB-A
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.

Dodavatel v rámci plnění Smlouvy zajistí následující rozhraní (zejména SQL dotazy, skripty), kterým budou výsledky monitorování předávány Zadavateli pro napojení do jím používaných systémů pro monitorování:

- Manageengine Application manager (https://www.manageengine.com/products/applications_manager/)
- Cacti (http://www.cacti.net)
- Oracle Enterprise manager (http://www.oracle.com/technetwork/oem/sys-mgmt/index.html)
- Icinga (https://www.icinga.com/)

1.3.1 Projektové vedení a eskalační proces

Zadavatel požaduje, aby se po celou dobu plnění scházel minimálně jednou za šest týdnů Řídící výbor (ŘV), jednou za šest týdnů Bezpečnostní výbor (BV) a jednou za 14 dní Výkonný výbor (VV), a to v budově Zadavatele. Bližší pravidla řízení projektu (jednotlivé řídící struktury včetně obsazení ŘV a BV, VV, odpovědnost, postupy odsouhlasení zápisů atd.) si smluvní strany dohodnou nejpozději do 1 měsíce od účinnosti Smlouvy. Účast na projektovém vedení (ŘV, BV, VV) se nevykazuje do výkazu za průběžný rozvoj, bezpečnost a údržbu DMS. Účast na jednání je zahrnuta v ceně měsíčního paušálního plnění.

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, bude tento předložen k řešení místně příslušnému soudu.

1.3.2 Zajištění projektové kanceláře a projektové dokumentace

Zadavatel je vlastníkem úplné projektové dokumentace. Aktuální dokumentace je platná podle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (VoKB).

Zadavatel aktuálně udržuje následující projektovou dokumentaci

- Technický popis infrastruktury DMS ČÚZK
- Uživatelská dokumentace DMS ČÚZK
- Uživatelská dokumentace DMS ČÚZK – admin
- Webové služby DMS ČÚZK
- Řízení přístupu k DMS ČÚZK
- Mapování metadat k typům dokumentu DMS ČÚZK
- Metadata k migraci přes Samba server DMS ČÚZK
- Dokumentace OB-TA
- Enterprise architektura DMS ČÚZK
- Analytický model DMS ČÚZK

Zadavatel požaduje, aby Dodavatel pro vedení dokumentace používal projektovou kancelář provozovanou Zadavatelem.

Zadavatel požaduje aktualizaci projektové dokumentace s každou změnou nasazenou na PROD prostředí. Zároveň Zadavatel požaduje provést aktualizaci projektové dokumentace dle požadavků na ISVS.

Základní charakteristiky práce s PK jsou uvedeny v Příloze Smlouvy S02.

Příloha S07 - Záruka

Požadavky na záruční servis

1.1 Základní parametry záručního servisu

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

1. záruční doba činí 2 roky od akceptace daného plnění, zároveň však nejdéle do konce uzavřené Smlouvy;
2. záruční servis bude poskytován v pracovní dny (od pondělí do pátku mimo státní svátky ČR) 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 začíná běžet od nahlášení v době záručního servisu (doručení zprávy do SD Dodavatele), popřípadě od následujících 6:00 v pracovní den pokud bylo nahlášení Dodavateli doručeno v době mimo hodiny záručního servisu;
3. poskytnutá záruka se vztahuje na všechny části díla, včetně příslušenství;
4. záruka se vztahuje na funkčnost díla, jakož i na vlastnosti požadované Zadavatelem;
5. záruka se prodlužuje o dobu, po kterou mělo dílo závadu bránící jeho řádnému užívání Zadavatelem;
6. 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;
7. 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;
8. 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;
9. Dodavatel odpovídá Zadavateli za případnou škodu, která mu vznikne z titulu neodstranění závady díla ve sjednaném termínu;
10. pro případy, kdy odstranění závady není ve sjednané lhůtě objektivně možné, navrhne Dodavatel Zadavateli náhradní řešení, které bude co nejvíce eliminovat případnou škodu Zadavatele;
11. pokud se Účastník zadávacího řízení rozhodne v DMS využít nekomerční (Open Source) SW, vztahuje se záruka i na něj.

1.2 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.

1.3 Klasifikace chyb / stupeň závažnosti

Každý Zadavatelem ohlášený požadavek kategorie „záruka“ 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 konzistence 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. 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. 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.

Stupeň závažnosti	Klasifikace chyby	Popis závady / dopad závady na činnosti Zadavatele
		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.

1.4 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

Příloha S08 – Podrobný popis metodiky vývoje

Dodavatel vyrábí systémy v souladu s relevantními standardy pro tvorbu software, včetně požadavků na kybernetickou bezpečnost (prováděcí vyhláška k ZoISVS).
Dodavatel je držitelem ISO certifikátů ISO 9001:15 Quality Management Systém, ISO/IEC 20000-1:18 IT Service Management – ITIL, ISO/IEC 27001:22 Information Security Management Systém, ISO/IEC 27701:19 Privacy Information Management Systém.
Při výrobě software vychází ze standardních metodik (Unified proces. Prince2Agile, Scrum, TOGAF, ITIL), 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 Projektovým zákonem je uspokojení požadavků zákazníka. Prostředkem k dosažení tohoto cíle je kromě samotného vývoje software řádná dokumentace projektu, důraz na otestování a finální akceptace zákazníkem.
Dodavatel 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. Vybrané pracovní postupy se liší s ohledem na charakter zakázek (implementační projekt, poskytování servisních služeb).
Následující kapitoly obsahují bližší informace metodických postupech.

1. Základní charakteristika Projektového zákona

Způsob a metodika vývoje je řízena interní metodikou **S018 – Projektový zákon**.
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**. **V případě poskytování servisních služeb je cílem dodržovat stanovená kritéria služeb (SLA).**
V průběhu řízení projektu vedoucí projektu organizuje vykonávání metodických kroků definovaných v jednotlivých fázích v souladu s potřebami projektu a metodickými nařízeními. Pro podporu činností jsou různé systémy (ISZA, IMIS, Sharepoint, MS-Project, Jira, EA,…).
Řízení projektu / zakázky zahrnuje níže uvedené oblasti:

- 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

Vlastní životní cyklus vývoje prochází jasně definovanými fázemi. V rámci těchto fází jsou specifikovány detailní postupy a výstupy. V následujícím textu jsou tyto kroky blíže popsány. Jedná se o:

- Fáze zahájení
- Fáze příprava
- Fáze konstrukce
- Fáze nasazení

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

2. Zpracování výstupů v rámci životního cyklu vývoje

V rámci životního cyklu vývoje jsou vytvářeny požadované výstupy. Pro jednotlivé výstupy jsou připraveny šablony a bližší metodická upřesnění. 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. Pro každý projekt je upřesněn rozsah zpracování výstupů v rámci fáze zahájení.

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

V dalším textu jsou uvedeny bližší informace pro tvorbu vybraných výrobních výstupů. Analytická dokumentace primárně vzniká v nástroji Enterprise Architect a je generována do formy dokumentů ANV. Tyto popisy jsou v udržovány aktuální, vetší část jich vzniká ještě před vlastním programováním a slouží jako jeho zadání.

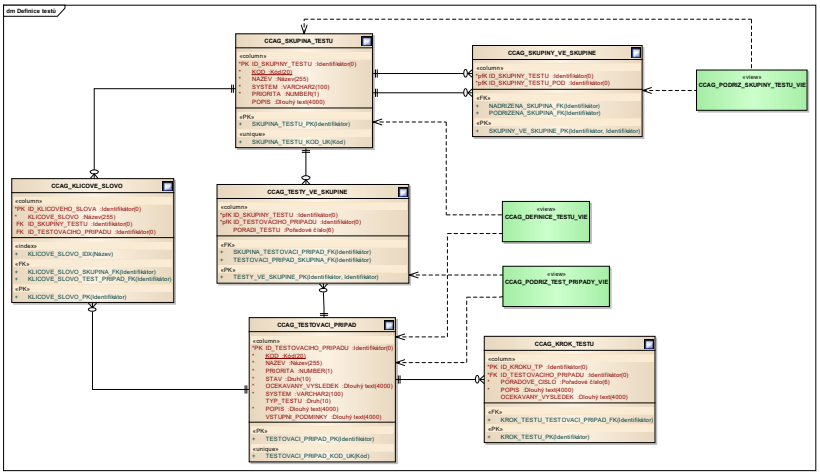
Databázové objekty:

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*
	CCAG_KROK_TESTU. *0..* Výsledek kroku.*
	*0..** *CCAG_KROK_TESTU.KROK_TESTU_TESTOVACI_PRIPAD_FK* *1* *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

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.

Instalační příručky:
Instalační příručky systémů jsou vytvářeny, 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.)

Zdrojový kód:
Zdrojový kód vzniká na základě stanovených metodických postupů (pojmenování, komentování) a je ukládán do 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. Vytvořený programový kód je podroben automatické statické analýze a code review, prováděnému seniorními SW inženýry. Součástí analýzy a review je také hodnocení bezpečnosti.

Interní testování:
Procesy interního testování popisuje dokument Metodika testování. 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. 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 se používá 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. Samozřejmou součástí jsou i testy na zajištění bezpečnosti. 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 integrální částí výrobního procesu.

3. Helpdeskový systém

Pro řízení zpracování požadavků a incidentů je využíván helpdeskový systém. Aplikace HelpDesk byla navržena podle best practices procesů ITIL a kombinuje uživatelský komfort na straně zákazníka a kompletní podporu procesů service desku na straně poskytovatele služby. Helpdesk je vždy konfigurován pro konkrétní požadavky daného projektu / zakázky.
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

Hlášení, proces jeho přijetí a zpracování:

Hlášení může být podáno Objednatelem 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 Objednateli 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 Objednatele 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 Objednatele k vyřešenému hlášení ve stanovené lhůtě nebo uplynutím této lhůty, pokud se Objednatel k vyřešenému hlášení nevyjádří.

Příloha S09 – Požadavky na způsob řízení projektu a personální zajištění Smlouvy

Projektové vedení a eskalační proces

Zadavatel požaduje, aby se po celou dobu plnění scházel minimálně jednou za šest týdnů 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 od účinnosti 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, bude tento předložen k řešení místně příslušnému soudu.

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 kybernetické bezpečnosti)	[redacted]

Příloha S10 – Propojení HD Zadavatele s HD Dodavatele

HD Zadavatele slouží pouze pro řešení hlášení. Neslouží pro potřeby testování. Informace o interní analýze na straně Dodavatele, sledování interních SLA a případném testování musí být evidovány v jiném systému.

Vytvoření hlášení

V HD ČÚZK musí být vytvořeno hlášení s následujícími parametry:

Povinné parametry:

- *Tenant - CUZK interni*.
- *Dodavatel* - název nového dodavatele Rozvoje a údržby DMS ČÚZK 2025-2030.
- *Stav* – Automaticky nastavený Přidělený
- *Kategorizace*.
    - Podle kategorizace je v HD dodavatele zakládán správný typ ticketu.
        - *Název nového dodavatele Dotaz* - při potřebě získat odpověď na položenou otázku v případě problému, u kterého si není objednavatel jist, že se jedná o Závadu, vykazován bude ve službách průběžné údržby,
        - *Název nového dodavatele Závada* – závada DMS ČÚZK, která musí být řešena, závada bude vykazována ve službách průběžné údržby, pokud se nejedná o záruční závadu ze Smlouvy.
        - *Název nového dodavatele Požadavek údržba* – požadavek na průběžnou údržbu DMS ČÚZK, vykazován bude ve službách průběžné údržby,
        - *Název nového dodavatele Požadavek rozvoj* – požadavek na rozvoj DMS ČÚZK, vykazován bude ve službách průběžného rozvoje,
        - *Název nového dodavatele Bezpečnost* – požadavek na bezpečnost DMS ČÚZK, vykazován bude v Bezpečnosti IS.
- *Priorita dodavatele*.
    - **Nejvyšší je priorita 1**.
    - …
    - **Nejnižší priorita 4.**

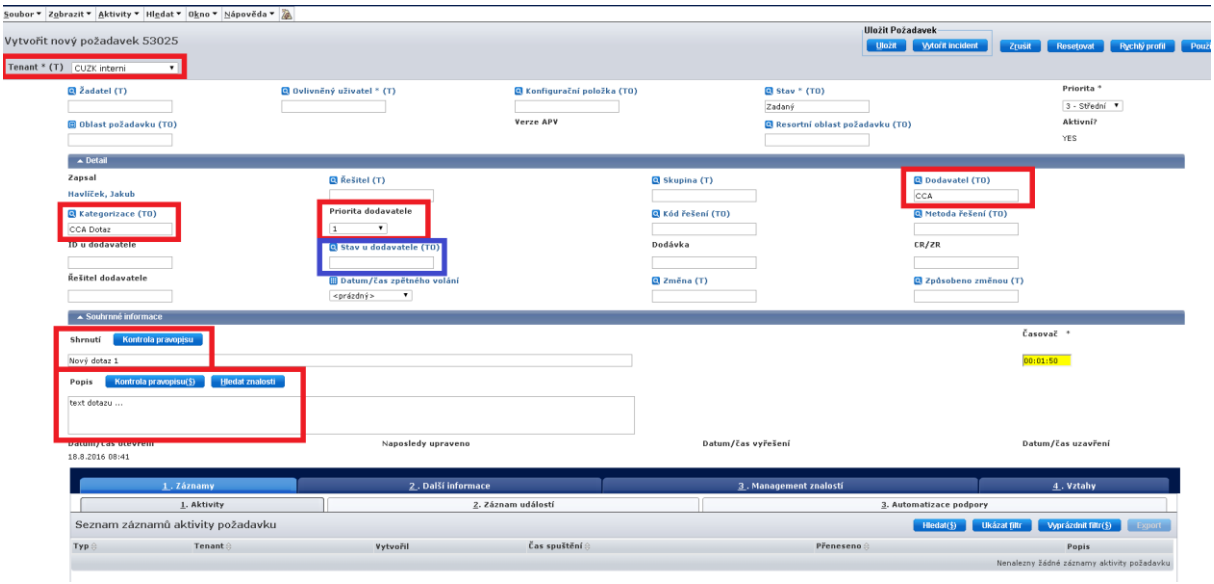
Stupeň závažnosti	Klasifikace chyby	Popis závady / dopad závady na činnosti Zadavatele
1	Kritická závada	DMS není použitelný ve svých základních funkcích nebo se vyskytuje funkční závada znemožňující práci s DMS z důvodu, že některá aplikace nebo její část je zcela nefunkční a požadovanou činnost nelze realizovat jinak, nebo stav DMS umožňuje porušení konzistence 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. 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. 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.

- *Shrnutí (Nadpis HD).*
- *Popis.*

Nepovinné parametry:

- *Příloha.*



Obrázek 1: Povinná pole

Dotazy, Rozvojové požadavky (údržba i rozvoj) a Požadavky na bezpečnost IS se zadávají s Prioritou dodavatele 3, pokud není dohodnuto v rámci vedení projektu Zadavatele i Dodavatele jinak.

Inicializace přenosu z HD Zadavatele do HD Dodavatele

Přenos do systému dodavatele je inicializován změnou stavu z *Přidělený* na *Řeší dodavatel* (tj. po vytvoření hlášení). Tuto změnu je oprávněn provést zaměstnanec Zadavatele uvedený v příloze ZD10 Metodika podpory DMS.

Do HD Dodavatele se přenesou minimálně následující pole:

- ID hlášení ČÚZK
- Shrnutí (Nadpis)
- Kategorizace hlášení
- Priorita dodavatele
- Popis hlášení
- Příloha (je-li součástí hlášení)

V této fázi dochází ke kontrole vyplnění jednotlivých polí. V případě chyb (pole není vyplněno, selhal přenos, …) je vrácen původní stav a chyba je zapsáno formou technického komentáře. Pouze pole pro přílohu nemusí být vyplněné (jedná se o volitelné pole). Ostatní přenášená pole jsou povinná.

Pokud je vše v pořádku odesláno do HD Dodavatele, odešle HD Dodavatele do HD Zadavatele dvě pole *ID u dodavatele* a *Stav u dodavatele*.

Jakmile začne dodavatel hlášení řešit, dojde ke změně stavu u dodavatele na *Název nového dodavatele V řešení*. Tato informace je opět odeslána do HD Zadavatele.

Přenos komentáře, dodatečného komentáře, či nové přílohy

Při vkládání komentáře, dodatečného komentáře, či přílohy k HD Zadavatele musí dojít k přenosu i tohoto komentáře/přílohy do HD Dodavatele – okamžitě po jeho uložení v HD Zadavatele.

Inicializace přenosu z HD Zadavatele do HD Dodavatele

K inicializaci přenosu HD Zadavatele do HD Dodavatele je oprávněný pouze zaměstnanec Zadavatele uvedený ve schválené příloze ZD10 Metodika podpory DMS.

Ze systému Dodavatele se do systému Zadavatele přenáší následující pole:

- ID hlášení u dodavatele
- Dodávka (plán dodavatele, do které verze, hotfixu bude hlášení zprovozněno). Data v poli Dodávka (HD Zadavatele zůstávají), v případě změny se hodnota přidává za původní (např. 1.1.4, 1.1.4.01, 1.1.4.04)
- CR (číslo analýzy, pod kterou je hlášení prováděno)
- Stav dodavatele (*Název nového dodavatele Přiděleno dodavateli, Název nového dodavatele V řešení, Název nového dodavatele Přerušeno součinnost, Název nového dodavatele Vyřešeno)*
- Komentář

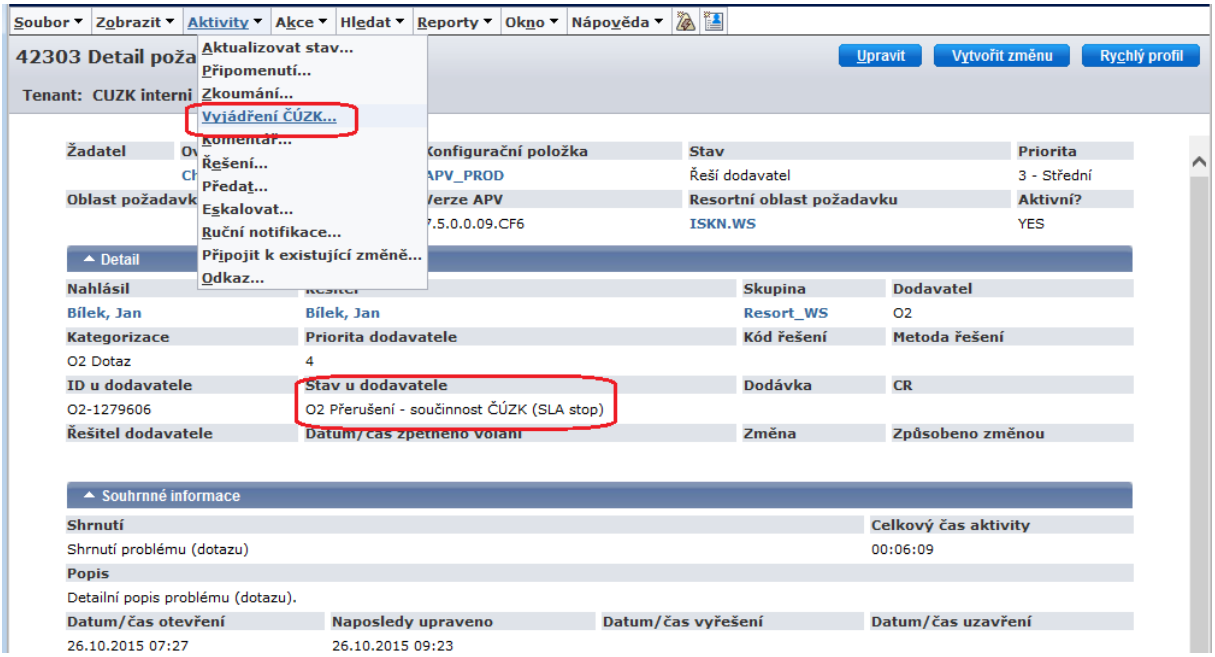
- Příloha

Reakce Zadavatele na Stav Dodavatele

Vyjádření ČÚZK

Vyjádření ČÚZK je oprávněn provést pouze zaměstnanec Zadavatele uvedený ve schválené příloze ZDMetodika podpory DMS.

V případě, kdy Dodavatel potřebuje zpětnou vazbu od ČÚZK (doplnění, vyjádření, …), přerušuje řešení hlášení a do HD Zadavatele je přenesen Stav u dodavatele *Název dodavatele Přerušeno součinnost*. Pro zpětnou vazbu je u požadavku k dispozici aktivita *Vyjádření ČÚZK*…, přes kterou je Dodavateli předána informace k součinnosti.



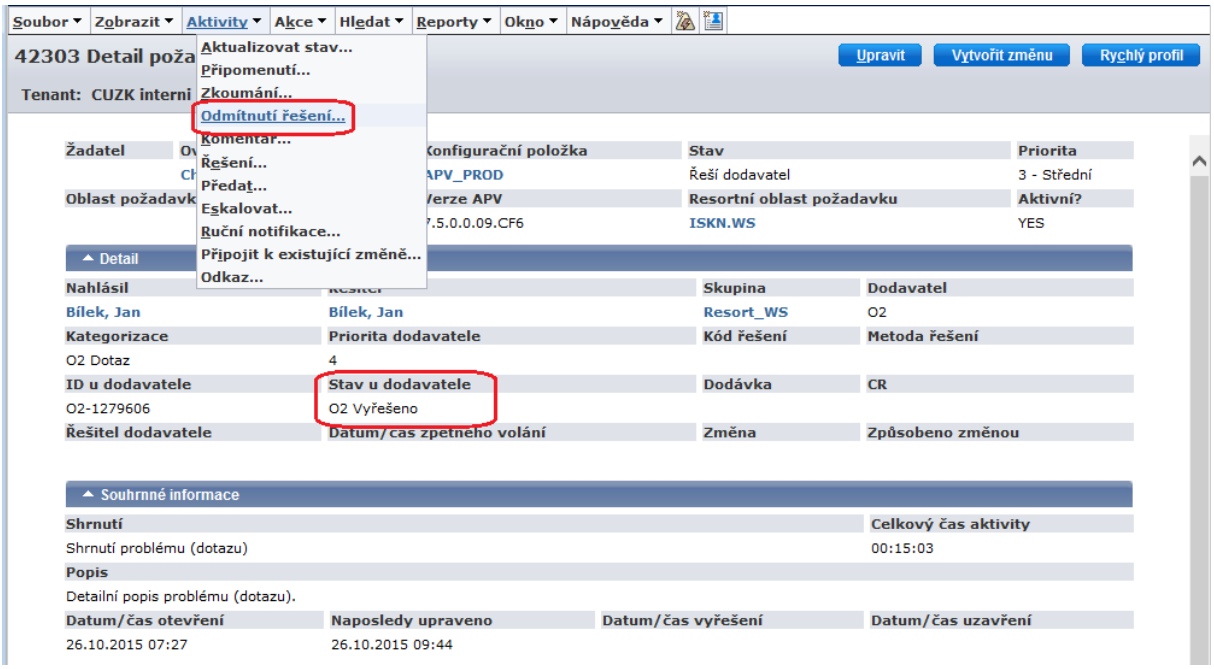
Obrázek 2: Vyjádření ČÚZK

Po vyplnění Vyjádření ČÚZK… je toto vyjádření opět okamžitě předáno do HD Dodavatele a opět začíná běžet SLA.

Odmítnutí řešení

Odmítnutí řešení je oprávněný provést pouze zaměstnanec Zadavatele uvedený v příloze ZD10 Metodika podpory DMS.

Pokud řešitel ČÚZK nesouhlasí s vyřešením hlášení (stav u dodavatele je *Nový dodavatel Vyřešeno*), může řešení odmítnout. K tomu je k dispozici aktivita *Odmítnutí řešení*… Po vyplnění Odmítnutí řešení se opět toto odmítnutí okamžitě předá do HD Dodavatele a opět začíná běžet SLA.



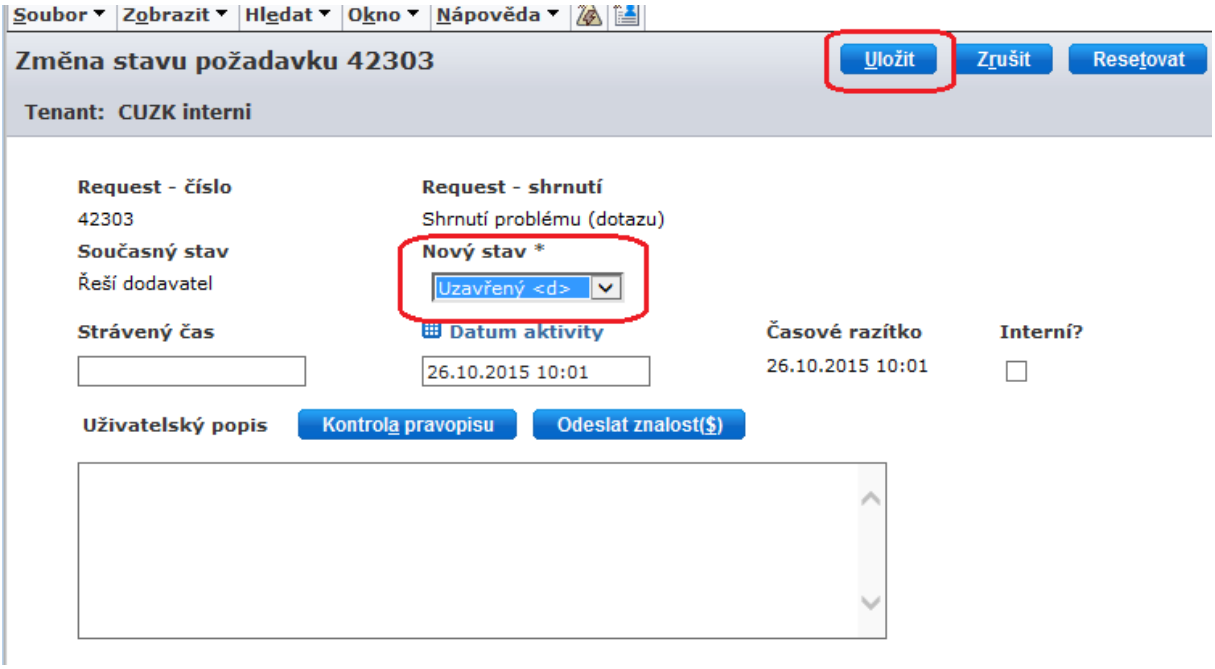
Obrázek 3: Odmítnutí řešení

Ukončení/uzavření hlášení

Ukončení/uzavření hlášení je oprávněný provést pouze zaměstnanec Zadavatele uvedený v příloze ZD10 Metodika podpory DMS.

Vyřešené hlášení je po uzavření v HD Zadavatele uzavřeno i v HD Dodavatele. Podmínkou vyvolání uzavření i v HD Dodavatele je, že *stav* je ***Řeší dodavatel***, *ID dodavatele* je vyplněné, *dodavatel* je Dodavatel.

V případě, že dojde k uzavření hlášení v HD na straně ČÚZK z jiného stavu než „Řeší dodavatel“, nedojde k automatickému uzavření hlášení v HD Dodavatele, uzavření je možné vyvolat opakovanou změnou v HD ze stavu ***Řeší dodavatel*** na ***Uzavřený***. Za uzavírání hlášení je zodpovědný zaměstnanec Zadavatele uvedený v příloze ZD10 Metodika podpory DMS.



Obrázek 4: Uzavření požadavku

Změna priority

Ke změně priority je oprávněný pouze zaměstnanec Zadavatele uvedený v příloze ZD10 Metodika podpory DMS. Při změně priority dochází k aktualizaci priority na straně Dodavatele. Informace o změně priority se přenáší z HD Zadavatele do HD Dodavatele. V aktivitách požadavku v HD je o změně priority v systému dodavatele záznam.

Změna kategorizace

Ke změně kategorizace je oprávněný pouze zaměstnanec Zadavatele uvedený v příloze ZD10 Metodika podpory DMS. Při změně kategorizace je o změně proveden záznam, který se přenáší z HD Zadavatele do HD Dodavatele. Změna kategorizace se děje na základě domluvy mezi Zadavatelem a Dodavatelem.

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.

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	http://hotline.cca.cz/
E-mail	hotline@cca.cz
Telefon	+420 378 229 455

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. Práce se zákaznickými hlášeními bude odpovídat dosavadním zavedeným postupům Dodavatele, včetně postupů krizové komunikace.

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 e-mailem 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 poskytovatele 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

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
- Nastavení lhůt řešení pro všechny druhy hlášení
- Přiřazení oprávněných řešitelů k hlášením a způsob notifikací

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 ČÚZK. Toto propojení bude provozováno i nadále po podpisu smlouvy na plnění servisu v letech 2025-2030.

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 ČÚZK, Odmítnutí řešení, Ukončení řešení, Změna priority či kategorie)

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