Příloha RD06 – Rozsah provozní údržby

č. sml. Objednatele: ČÚZK-12466/2018 -24 č. sml. Zhotovitele: B181228

1 Úvod

Provozní údržba (PÚ) znamená řešení a odstraňování provozních problémů a havárií ISKN tak, aby nebyl v žádném okamžiku ohrožen řádný výkon státní správy v oblasti katastru nemovitostí.

PÚ je hrazena měsíčním paušálním poplatkem a zahrnuje:

1.1 Identifikaci požadavku

Identifikací požadavku se rozumí analýza příčin problému nahlášeného Objednatelem.

1.2 Kategorizaci požadavku

Kategorizací požadavku, v návaznosti na identifikaci, se rozumí stanovení, zda jde o:

- záruční vadu,
- drobnou úpravu,
- činnost na objednávku (rozsahem přesahuje drobnou úpravu a nebude tedy řešena v rámci PÚ).

1.3 Odhad pracnosti v ČLD

Odhad pracnosti v ČLD pro řešení drobné úpravy.

1.4 Vyřešení požadavku

Vyřešením požadavku se rozumí zejména následující činnosti Zhotovitele:

- vypracování analýzy a návrhu řešení,
- implementace dle Objednatelem odsouhlaseného návrhu řešení, včetně případné úpravy dat,
- provedení interního otestování,
- předání úpravy Objednateli k testování,
- zařazení úpravy do příslušné verze ISKN (dodávka nové verze ISKN nebo opravný patch),
- předání opravného skriptu či oprav kritických, závažných nebo bezpečnostních chyb urychleně bez vazby na dodávku ISKN.

Kritické chyby budou řešeny se stejným SLA jako kritické chyby spadající do záručního servisu, viz Příloha RD05.

1.5 Činnosti v oblasti bezpečnosti

1.5.1 Činnosti Zhotovitele/Specialisty kybernetické bezpečnosti

Specialista kybernetické bezpečnosti Zhotovitele dle VoKB zastává pro ISKN roli:

- Manažer kybernetické bezpečnosti VIS ISKN,
- Architekt kybernetické bezpečnosti VIS ISKN.

Uvedené role, včetně povinností, které z těchto rolí vyplývají, jsou uvedeny v Příloze RD03. Tyto role mohou zastávat dvě osoby Zhotovitele, přičemž obě tyto osoby musí splňovat kvalifikační požadavky na Specialistu kybernetické bezpečnosti.

1.5.2 Oblast dokumentace

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

- dle ZoISVS vyhodnotit dodržování Informační koncepce informačních systémů veřejné správy resortu zeměměřictví a katastru (části týkající se ISKN), stanovit závěry z vyhodnocení a navrhnout opatření, která budou přijata k odstranění nedostatků, a to formou zápisu o vyhodnocení,
- dle ZoISVS aktualizovat a nadále udržovat aktuální provozní dokumentaci ISKN,
- dle ZoKB a VoKB aktualizovat a nadále udržovat aktuální bezpečnostní dokumentaci o prováděných bezpečnostních opatřeních v ISKN,
- vytvořit a nadále udržovat aktuální dokument popisující řízení přístupu interních a externích uživatelů DP ISKN,
- vytvořit a nadále udržovat aktuální dokument uvádějící minimální rozsah oprávnění interních uživatelů ISKN potřebných pro výkon práce na daném systemizovaném místě a organizační jednotce resortu ČÚZK.

1.5.3 Další činnosti

Další činnosti v oblasti bezpečnosti

- sledovat zejména:
  - Informační servis Národního úřadu pro kybernetickou a informační bezpečnost,
  - security bulletiny/advisory společností, jejichž SW se v ISKN využívá (Oracle, Microsoft atd.),
  - další zdroje zabývající se zveřejňováním zranitelností,

  a pravidelně Objednatele informovat o možných relevantních hrozbách a zranitelnostech souvisejících s ISKN a navrhovat opatření na jejich eliminaci,
- navrhovat změny (zlepšení) v oblasti bezpečnosti ISKN,
- z hlediska bezpečnosti průběžně sledovat a kontrolovat projednávané změny a úpravy ISKN (analýzy a návrhy řešení) a navrhovat případné úpravy,
- pro oblasti zasažené/měněné v dodávce ISKN provádět z hlediska bezpečnosti kontrolu architektury a kódu (code review),
- při každé změně ISKN předat do měsíce aktualizaci havarijních plánů (tj. plánů obnovy) ISKN včetně postupů při obnově provozu ISKN,
- do jednoho měsíce od začátku účinnosti RD a v souladu s čl. 11.9 RD vytvořit a udržovat aktuální dokument popisující zajištění bezpečnosti (organizační i technická opatření) projektové kanceláře Zhotovitele včetně řízení přístupu k ní,
- do jednoho měsíce od začátku účinnosti RD 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 Zhotovitele, tak mezi Zhotovitelem a Objednatelem, a to se zohledněním stupňů důvěrnosti dle bodu 1.5.4, a tento způsob zajistit,
- trvale zajišťovat bezpečnost informací a bezpečnost činností při vlastním plnění Zhotovitele (zabezpečení infrastruktury, postupů, ochrany dat apod.),
- svolávat minimálně 1x za 2 měsíce v sídle Objednatele jednání k zajištění bezpečnosti ISKN a pořizovat z nich zápisy. Na jednáních informovat o aktuálním stavu plnění činností, úkolů,

konzultovat spolu se zástupcem Objednatele problémy, předkládat návrhy na zlepšení bezpečnosti, předkládat k připomínkám návrhy/aktualizace dokumentů aj.,

- průběžně zajišťovat aktuálnost dokumentů týkajících se bezpečnosti uvedených v Příloze RD15.

1.5.4 Stupně důvěrnosti informací

Všechny informace týkající se předmětu plnění (dále též jen „informace") bude Zhotovitel klasifikovat a přidělovat jim následující stupně důvěrnosti:

- Veřejné – informace, jejichž zveřejnění nenaruší bezpečnost informací v resortu ČÚZK.
- Interní – informace, jejichž zveřejnění mimo resort ČÚZK by mohlo narušit bezpečnost informací, jsou určeny pouze pro zaměstnance Objednatele nebo Zhotovitele.
- Diskrétní – informace, se kterými se smí seznamovat pouze určený okruh osob.
- Přísně diskrétní – informace vyžadující nejvyšší stupeň ochrany a mohou se s nimi seznamovat pouze přesně určené fyzické osoby, přístup k těmto informacím podléhá písemné evidenci.

Informace bez označení stupně důvěrnosti bude klasifikována jako „interní". Objednatel má právo stupeň důvěrnosti v odůvodněných případech překlasifikovat, a to v součinnosti se Zhotovitelem.

1.5.5 Oblast bezpečnostních testů

Zhotovitel bude provádět bezpečnostní testy ISKN vždy před předáním dodávky nové verze nebo hotfixu/patche ISKN a to minimálně v rozsahu Přílohy RD08.

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 Objednatelem.

K minimalizaci rizik spojených s možnými chybami při vývoji externích aplikací bude Zhotovitel při vývoji používat nástroj pro kontrolu bezpečnosti např. Netsparker, Burp suite professional, Acunetix, Metasploit, Nessus.

1.5.6 Proaktivní zajišťování bezpečnost ISKN

Zhotovitel bude průběžně proaktivně navrhovat Objednateli změny (zlepšení) v oblasti bezpečnosti ISKN na základě aktuálních trendů v oblasti kybernetické bezpečnosti a na základě nejlepší praxe v oblasti bezpečnosti informací popsané sadou norem ISO 27000. Zhotovitel se zavazuje, že poznatky, získané pracovníky jeho realizačního týmu na základě své praxe, účastí na pravidelných školeních, workshopech a konferencích (např. konference pořádané NÚKIB, ISACA, školení technologie Fidelis Cybersecurity, aj.), bude promítat do svého plnění.

Vlastní forma a frekvence proaktivního informování bude definována a odsouhlasena v rámci standardních projektových postupů.

1.6 Monitorování provozu ISKN

1.6.1 Obecné zásady

Minimálně v období 3 pracovních dnů následujících po instalaci změn ISKN do produkčního prostředí, případně až do vyřešení zjištěných problémů, bude Zhotovitel provádět monitorování provozu ISKN. Monitorovány musí být zejména části ISKN, které byly v rámci dané verze modifikovány (modifikací se rozumí i zavedení nové funkčnosti), nebo části, které nebyly modifikovány, ale mohou být úpravami přímo nebo nepřímo ovlivněny.

Výsledky monitorování provozu budou vzájemně odsouhlaseným způsobem v dohodnutých časových intervalech předávány Objednateli. U nově zaváděných funkčností zároveň Zhotovitel předá Objednateli popis provozního monitorování (sledované metriky, způsob získávání metrik, jejich meze, typické intervaly sledování, reakce na mezní hodnoty). Zhotovitel bude dále v rámci monitorování upozorňovat Objednatele na problémy (nefunkčnost, úzká místa atd.), která při monitorování zjistil. U problémů, které mohou ohrozit funkčnost ISKN, bude Zhotovitel upozorňovat Objednatele bezodkladně.

1.6.2 Popis monitorování provozu ISKN

Pro realizaci monitoringu provozu ISKN budou předána přístupová práva k monitorovacím nástrojům Objednatele, monitorujícím prostředí Objednatele, která jsou předmětem monitoringu, v rozsahu nezbytném pro provádění monitoringu provozu Zhotovitelem.

V odůvodněných případech bude poskytnut i přístup přímo k monitorovaným prostředím (výhradně s právy pouze pro čtení), pokud nelze požadované metriky získat z monitorovacích nástrojů Objednatele. Tímto se rozumí např. ad hoc dotazy do databáze za účelem sledování a vyhodnocování činnosti aplikace.

Zhotovitel písemně specifikuje Objednateli rozsah přístupových práv, které nezbytně potřebuje získat pro monitoring v rámci období, kdy provoz monitoruje Zhotovitel.

Technické podrobnosti a další organizační upřesnění způsobu zajištění monitorování provozu ISKN budou součástí standardních projektových dokumentů.

1.7 Zajištění podpůrných a souvisejících činností s plněním RD

Zajištěním všech podpůrných a souvisejících činností s plněním RD se rozumí např.:

- podpora při instalaci změn ISKN do referenčního a produkčního prostředí,
- vedení a administrace projektu,
- zajištění online dostupného zabezpečeného úložiště (viz čl. 11.8 RD),
- zřízení, zdokumentování a vedení projektové kanceláře (viz čl. 11.9 RD),
- zajištění a zdokumentování propojení HD systémů (viz čl. 11.10 RD),
- zajištění a zdokumentování podpory testování (viz čl. 11.11 RD),
- komunikace s Objednatelem, účast na schůzkách, součinnost s třetími stranami apod.