Příloha RD06 – Rozsah provozní údržby

č. sml. Objednatele: ČÚZK- 41763/2022  č. sml. Zhotovitele: CZBAP-1746

# 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:

## Identifikaci požadavku

Identifikací požadavku se rozumí analýza příčin problému nahlášeného Objednatelem.

## 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).

## Odhad pracnosti v ČLD

Odhad pracnosti v ČLD pro řešení drobné úpravy.

## 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.

## Činnosti v oblasti bezpečnosti

### 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.

### 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,
* udržovat aktuální dokument popisující řízení přístupu interních a externích uživatelů DP ISKN,
* vytvořit a udržovat aktuální dokument uvádějící minimální rozsah oprávnění interních uživatelů ISKN potřebných pro výkon práce na daném systemizovaném místě a organizační jednotce resortu ČÚZK.

### 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,
* posuzování dopadu změn do kybernetické bezpečnosti, hodnocení rizik změn,
* 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 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.

### 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.

### 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 a nebo 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.

### Proaktivní zajišťování bezpečnost ISKN

Zhotovitel bude sledovat zejména:

* Informační servis Národního úřadu pro kybernetickou a informační bezpečnost,
* security bulletiny/advisory, jejichž SW se v ISKN využívá (Oracle, Microsoft atd.),
* další zdroje zabývající se zveřejňováním zranitelností,
* a pravidelně Objednatel informovat o možných relevantních hrozbách a zranitelnostech souvisejících s ISKN a navrhovat opatření na jejich eliminaci.

Zhotovitel v průběhu plnění RD bude průběžně sledovat Informační servis Národního úřadu pro kybernetickou a informační bezpečnost, aktuality z bezpečnosti Národního CSIRTu České republiky a z dalších relevantních zdrojů jako například: HK CERT Infosec Express, MicroSoft Latest Security Advisories, Microsoft MSRC, Oracle Technology Network - Critical Patch Updates, aj. O případných zranitelnostech a hrozbách či bezpečnostních problémech a chybách, které by mohly mít dopad na ISKN, informuje pravidelně (cca 1x za 14 dní) prostřednictvím e-mailu kontaktní osoby Objednatele s popisem zranitelnosti a s návrhem opatření. Zhotovitel v průběhu plnění RD bude proaktivně rozšiřovat informační zdroje o případné další, které budou vzhledem k ISKN relevantní.

Zhotovitel dále bude:

* 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) prostřednictvím nástroje SonarQube, kontroluje vedoucí vývoje při respektování kontroly zdravého kódu, a penetračními testy.
* Při každé změně ISKN předávat do měsíce aktualizaci havarijních plánů (tj. plánů obnovy) ISKN včetně postupů při obnově provozu ISKN.
* Do jednoho měsíce od začátku účinnosti RD vypracuje a bude 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 požadavku Objednatele.

Zhotovitel bude:

* 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 bude 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.

Zhotovitele bude v průběhu plnění RD 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. Za tímto účelem se pracovníci realizačního týmu účastní pravidelných školení, workshopů a konferencí (např. konference pořádané NÚKIB, ISACA, školení technologií aj.). Zhotovitel se zavazuje, že poznatky a nejlepší praxi získané na základě těchto činností bude promítat do svého plnění.

## Monitorování provozu ISKN

### 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.

### Popis monitorování provozu ISKN

Při realizaci rozšíření monitoringu budou implementovány hladiny pro varování a pro závažný stav. Na tyto hladiny bude monitoring Objednatele reagovat zasíláním notifikací, a to na stanovenou skupinu uživatelů určenou pro danou oblast ISKN. Objednatel tak bude automaticky upozorňován na problémy hlídané implementovanými metrikami.

Pokud Objednatel umožní přístup k monitorovacímu nástroji produkčního prostředí, bude Zhotovitel sledovat údaje v tomto nástroji v průběhu stanoveného monitorovacího období.

Pokud dojde k vzájemnému dohodě, bude Zhotovitel doplněn mezi adresáty notifikací monitoringu produkčního prostředí ISKN. Zhotovitel nebude provádět monitorování produkčního prostředí vlastními automatizovanými prostředky.

Před zahájením monitorování stanoví Zhotovitel seznam oblastí, které bude pro danou dodávku zapotřebí monitorovat. Pro oblasti, pro které není stanovena žádná metrika, bude po vzájemné dohodě stanovena úroveň pro kritické stavy a konkrétní metoda, jakým bude měřená hodnota získávána. Domluvená úroveň a metoda pro měření budou poté užity při vyhodnocování naměřených hodnot.

Zhotovitel bude pro provádění používat manuální prostředky a monitoring Objednatele. V případě, že Zhotovitel objeví v průběhu monitorování nový typ problému, upozorní na to Objednatele. U problémů, které by mohly ohrozit funkčnost ISKN, bude Zhotovitel upozorňovat Objednatele bezodkladně.

## 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 a zdokumentování propojení HD systémů (viz čl. 11.9 RD),
* zajištění a zdokumentování podpory testování (viz čl. 11.10 RD),
* komunikace s Objednatelem, účast na schůzkách, součinnost s třetími stranami apod.