Příloha SML06 – Rozsah provozní údržby

č. sml. Objednatele: ČÚZK-20194/2021

1. Úvod

Provozní údržba (PÚ) znamená zejména řešení a odstraňování provozních problémů a havárií tak, aby nebyl v žádném okamžiku ohrožen výkon činností IS DMVS.

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,
- mimozáruční vadu,
- chybu z testování,
- 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, činnosti na objednávku a mimozáruční vady.

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 IS DMVS (dodávka nové verze IS DMVS nebo opravný patch).

Kritické chyby a závažné chyby budou v rámci PÚ řešeny se stejným SLA jako kritické chyby spadající do záruky, viz Příloha SML05.

1.5. Činnosti v oblasti bezpečnosti

1.5.1. Činnosti Zhotovitele/Specialisty kybernetické bezpečnosti

Specialista kybernetické bezpečnosti Zhotovitele dle VoKB zastává pro IS DMVS roli:

- Manažer kybernetické bezpečnosti
- Architekt kybernetické bezpečnosti.

Uvedené role, včetně povinností, které z těchto rolí vyplývají, jsou uvedeny v Příloze SML03. Tyto role mohou zastávat dvě osoby Zhotovitele, přičemž obě tyto osoby musí splňovat požadavky na Specialistu kybernetické bezpečnosti.

1.5.2. Oblast dokumentace

Objednatel požaduje, aby Zhotovitel při celkové akceptaci plnění a dále 1x ročně:

- dle ZoISVS vyhodnotil dodržování Informační koncepce informačních systémů veřejné správy resortu zeměměřictví a katastru (části týkající se IS DMVS), stanovil závěry z vyhodnocení a navrhl opatření, která budou přijata k odstranění nedostatků, a to formou zápisu o vyhodnocení,

- dle ZoISVS aktualizoval a nadále udržoval aktuální provozní dokumentaci IS DMVS,
- dle ZoKB a VoKB předal a nadále udržoval aktuální bezpečnostní dokumentaci IS DMVS dle Přílohy SML14.

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 IS DMVS využívá
  - další zdroje zabývající se zveřejňováním zranitelností,

  a pravidelně Objednatele informovat o možných relevantních hrozbách a zranitelnostech souvisejících s IS DMVS navrhovat opatření na jejich eliminaci,
- navrhovat změny (zlepšení) v oblasti bezpečnosti IS DMVS,
- z hlediska bezpečnosti průběžně sledovat a kontrolovat projednávané změny a úpravy IS DMVS (analýzy a návrhy řešení) a navrhovat případné úpravy,
- pro oblasti zasažené/měněné v dodávce IS DMVS provádět z hlediska bezpečnosti kontrolu architektury a kódu (code review),
- při každé změně IS DMVS předat do měsíce aktualizaci havarijního plánu (tj. plánů obnovy) IS DMVS včetně postupů při obnově provozu IS DMVS,
- do jednoho měsíce od začátku účinnosti Smlouvy a v souladu s čl. 11.9 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 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 Zhotovitele, tak mezi Objednatelem a Zhotovitelem, 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 IS DMVS 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 SML14.

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.
- Interní – informace, jejichž zveřejnění mimo Objednatele 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; 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“.

1.5.5. Oblast bezpečnostních testů

Zhotovitel bude provádět bezpečnostní testy IS DMVS před předáním plnění k celkové akceptaci a dále vždy před předáním dodávky nové verze nebo hotfixu/patche IS DMVS, a to minimálně v rozsahu dle Přílohy SML07.

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.

1.5.6. Proaktivní zajišťování bezpečnosti IS DMVS

Zhotovitel má zavedená opatření v rámci vlastního Systému řízení bezpečnosti (dále jen „ISMS“) a uplatní je na veškeré činnosti prováděné pro Objednatele. Zhotovitel bude uplatňovat požadavky politiky a procesy Objednatele na všechny činnosti při plnění předmětu díla. Pokud by vznil v bezpečnostních požadavcích interního ISMS Zhotovitele a bezpečnostními požadavky Objednatele případný rozpor, přednost má přísnější požadavek.

1.5.6.1. Bezpečnostní politika

Zhotovitel má stanovenu bezpečnostní politiku v rámci vlastního Systému řízení bezpečnosti informací. Politika je udržována aktuální, o změnách jsou informováni zaměstnanci. S obsahem politiky jsou seznamováni zaměstnanci při nástupu, politika je zahrnuta do Plánu zvyšování bezpečnostního povědomí.

Při plnění předmětu díla Zhotovitel uplatňuje současně politiky Objednatele. Plněny jsou požadavky politik Zhotovitele i Objednatele. S relevantními politikami jsou seznámeni všichni zaměstnanci Zhotovitele, i subdodavatelů, kteří se podílí na plnění zakázky.

1.5.6.2. Řízení aktiv

Zhotovitel v rámci svého systému řízení bezpečnosti informací udržuje přehled primárních a podpůrných aktiv. Automaticky sem patří činnosti vykonávané ve prospěch zákazníka, informace poskytnuté zákazníkem, informace vytvářené pro zákazníka, dokumentace, zdrojové kódy, záznamy související s plněním zakázky, interní informace Zhotovitele, výstupy, včetně dodávaného SW, technická aktiva využívaná pro plnění předmětu zakázky, zaměstnanci, dodavatelé.

Zhotovitel má stanoveny podmínky použití aktiv, požadavky a postupy pro vracení aktiv, klasifikaci a označování informací, manipulaci s aktivy, správu výměnných médií, likvidaci médií a jejich přepravu.

Pro účely projektu IS DMVS bude označování informací v souladu s pravidly Objednatele dle zadávací dokumentace (ZD 4.1.5.1).

Zhotovitel pro řízení aktiv IS DMVS vytvoří dokument „Metodika pro identifikaci a hodnocení aktiv a pro hodnocení rizik“ dle požadavku z přílohy Příloha ZD12-Seznam bezpečnostních dokumentů IS DMVS a to v souladu s metodikou Objednatele uvedenou v Příloze Příloha ZD11-Seznam bezpečnostních dokumentů ČÚZK. Pomocí již zavedených procesů v souladu s § 4 VoKB Zhotovitel zajistí dle této metodiky pro IS DMVS identifikaci a hodnocení aktiv, jejich garantů, vazeb, přípustného používání a likvidaci.

1.5.6.3. Řízení rizik

Zhotovitel má zaveden proces řízení rizik podle normy ISO 27005. Hodnocení rizik provádí alespoň 1x za rok. Zhotovitel má vytvořeny a zavedeny plány zvládání rizik. Realizována jsou opatření na základě právních požadavků, smluvních závazků, obchodních požadavků/osvědčených postupů a výsledků hodnocení rizik.

Zhotovitel bude pro hodnocení rizik IS DMVS používat Metodiku pro identifikaci a hodnocení aktiv uvedenou v příloze Příloha SML14 a bude zpracovávat a aktualizovat plán zvládání rizik.

1.5.6.4. Organizační bezpečnost

Zhotovitel má stanoveny požadavky na bezpečnost informací v dodavatelských vztazích a řízení dodávek služeb dodavatelů, vyhodnocuje rizika a implementuje opatření, stanovuje bezpečnostní požadavky v dohodách s dodavateli, monitoruje a přezkoumává služby dodavatelů, a řídí změny ve službách dodavatelů. V rámci plnění předmětu zakázky uplatní jak své požadavky, tak požadavky Objednatele dle Politiky řízení dodavatelů.

1.5.6.5. Řízení dodavatelů

Zhotovitel má stanoveny požadavky na bezpečnost informací v dodavatelských vztazích a řízení dodávek služeb dodavatelů, vyhodnocuje rizika a implementuje opatření, stanovuje bezpečnostní požadavky v dohodách s dodavateli, monitoruje a přezkoumává služby dodavatelů, a řídí změny ve službách dodavatelů. V rámci plnění předmětu zakázky uplatní jak své požadavky, tak požadavky Objednatele dle politiky řízení dodavatelů.

1.5.6.6. Bezpečnost lidských zdrojů

Zhotovitel v rámci vlastního systému řízení bezpečnosti informací prověřuje uchazeče o zaměstnání, v pracovních smlouvách stanovuje podmínky týkající se bezpečnosti informací, má zaveden plánem rozvoje bezpečnostního povědomí, a zavedena opatření při ukončení nebo změně pracovního vztahu. Zhotovitel zajistí seznámení všech zaměstnanců, podílejících se na plnění zakázky, jakož i subdodavatelů, s požadovanými a realizovanými opatřeními na zajištění bezpečnosti informací při plnění předmětu zakázky včetně případných změn.

1.5.6.7. Řízení provozu a komunikací

Zhotovitel bude udržovat provozní dokumentaci podle požadavků § 10 VoKB a ZD. Popsány budou všechny provozní činnosti tak, aby bylo minimalizováno riziko chyby. V rámci plnění požadavků VoKB Zhotovitel zajistí oddělení vývojového, testovacího a provozního prostředí.

1.5.6.8. Řízení změn

Zhotovitel zajistí v rámci provozu podklady pro přezkoumání možných dopadů změn a jejich vyhodnocení, zda se jedná o významnou změnu. Všechny změny budou dokumentovány, v případě významných změn bude zajištěno plnění § 11 VoKB, a to zejména analýza rizik, návrhy opatření, aktualizace politik a dokumentací, testování zranitelností a penetrační testování. Zhotovitel při řešení zranitelností a jejich evidenci využívá nástroj pro řízení implementace zákaznických požadavků JIRA.

1.5.6.9. Řízení přístupu

Zhotovitel zajistí řízení přístupu k veškerým informacím souvisejícím s plněním předmětu zakázky ze strany vlastních zaměstnanců, subdodavatelů a zaměstnanců Objednatele. Zhotovitel má stanovenu a přísně dodržuje politiku řízení přístupu, uplatňován je princip, že každý má pouze takový přístup, který nutně potřebuje pro plnění stanovených úkolů, a to jak vůči vlastním zaměstnancům, tak vůči externím subjektům, je řízen přístup k sítím a síťovým službám, aplikována pravidla pro registraci a zrušení registrace uživatele, správu uživatelských přístupů, správu privilegovaných přístupů, správu autentizačních dat a předmětů, přezkoumávání přístupových oprávnění, a odebírání a úpravu oprávnění. Aplikována budou opatření požadovaná Objednatelem.

V rámci údržby IS DMVS budeme aplikovat požadavky § 12 VoKB.

1.5.6.10. Akvizice, vývoj, údržba

Zhotovitel zajistí stanovování bezpečnostních požadavků na změny IS DMVS spojené s jeho akvizicí, vývojem a údržbou a uplatňování jejich zahrnutí do projektu, jehož součástí je akvizice, vývoj a údržba IS DMVS, v rámci výkonu bezpečnostních rolí podle kap. 5.3.2 Činnosti specialisty kybernetické bezpečnosti, prováděné v rámci paušálu.

1.5.6.11. Zvládání kybernetických bezpečnostních událostí a incidentů

Zhotovitel má v rámci vlastního Systému řízení bezpečnosti informací stanoveny postupy a odpovědnosti pro hlášení událostí, hlášení slabých míst, rozhodování o incidentu, reakci na incident, ponaučení z incidentu a shromažďování důkazů.

V rámci výkonu rolí Manažer kybernetické bezpečnosti a Architekt kybernetické bezpečnosti budou vykonávány činnosti související s incidenty kybernetické bezpečnosti uvedené v kapitole 5.3.2 Činnosti specialisty kybernetické bezpečnosti prováděné v rámci měsíčního paušálu. Tyto činnosti budou přímo napojeny na procesy Zhotovitele.

1.5.6.12. Řízení kontinuity činností

Zhotovitel v rámci zajištění výkonu role bude:

- vytvářet a pravidelně aktualizovat dokument „Strategie řízení kontinuity činností“ pro IS DMVS
- ve spolupráci s manažerem kybernetické bezpečnosti IS DMVS a garantem aktiv IS DMVS zajišťovat minimálně 1x ročně aktualizace a otestování plánů obnovy IS DMVS
- navrhovat opatření pro zvýšení odolnosti IS DMVS vůči kybernetickým incidentům s využitím technických nástrojů pro zajišťování stanovené úrovně dostupnosti.

1.5.6.13. Audit kybernetické bezpečnosti

Zhotovitel má zaveden interní Plán auditů, který obsahuje jednotlivé projekty Zhotovitele. V rámci těchto auditů je kontrolována shoda s požadavky interního ISMS Zhotovitele a soulad s plněním požadavků Objednatele. Výsledky interních auditů předmětu plnění této zakázky budou předkládány Objednateli.

Zhotovitel bude prostřednictvím role Manažer kybernetické bezpečnosti IS DMVS poskytovat součinnost auditorovi kybernetické bezpečnosti a auditorům Objednatele při provádění auditů a kontrol, jakož i zajišťovat audit implementace schválených bezpečnostních opatření.

1.5.6.14. Fyzická bezpečnost

Přístupy do prostor Zhotovitele podléhají řízení přístupů, a to podle jednotlivých úrovní hodnocení aktiv. Přístup je kontrolován od zajištění ochrany na úrovni objektů až po úroveň přístupu k jednotlivým aktivům. Přístup je řízen politikou fyzické bezpečnosti Zhotovitele. Je stanovený fyzický bezpečnostní perimetr s definicí úrovní zabezpečených oblastí. Jsou stanoveny fyzické kontroly vstupu. Zaměstnanci společnosti ACE jsou vybaveni přístupovými kartami a příslušnými přístupovými právy pro vstup do prostor organizace. Návštěvy musí být ohlášeny a v prostorách firmy se smí pohybovat pouze v doprovodu zaměstnanců. Technologické oblasti tvoří samostatné prostory, ve kterých jsou ve zvýšené míře zpracovávány informace nebo je v nich zařízení IT vyšší hodnoty. Technologické zóny jsou odděleny od kancelářských oblastí fyzickým bezpečnostním perimetrem a každá oblast je zabezpečena samostatnou zónou elektronického zabezpečovacího systému (EZS) s prostorovou detekcí pohybu osob (PIR čidla) a detekcí požáru (EPS čidla); vybrané zóny EZS jsou deaktivovány pouze zaměstnanci s oprávněním vstupu do oblasti. Zaměstnanci deaktivují zónu EZS jen na dobu své přítomnosti v oblasti. Do technologických prostor ACE mohou vstupovat pouze zaměstnanci, kteří byli pověřeni výkonem činností v těchto prostorách (oprávnění zaměstnanci ACE). Jiné osoby mohou do těchto prostor vstupovat pouze za doprovodu oprávněného zaměstnance ACE. Mezi technické zabezpečovací prostředky používané Zhotovitelem patří také EPS, EZS, CCTV, ACS, skartovací zařízení a další.

1.5.6.15. Bezpečnost komunikačních sítí

Zhotovitel má zajištěnu a implementovánu ochranu bezpečnosti komunikační sítě. Komunikační síť je segmentována a vzdálený přístup je možný pouze při využití kryptografických prostředků a 2FA autentizace. Zhotovitel zajistí splnění požadavků VoKB a požadavků ZD při návrhu IS DMVS. V rámci bezpečnosti komunikačních sítí bude zajištěna jejich segmentace. Komunikace budě řízena jak v rámci sítě, tak na jejím perimetru. Důvěrnost a integrita komunikační sítě bude zajištěna pomocí autentizace a využití kryptografie. Pro zajištění segmentace sítě a pro řízení komunikace mezi jejími segmenty bude využíván nástroj, který zajistí ochranu integrity komunikační sítě.

1.5.6.16. Správa a ověřování identit

Zhotovitel má implementován centralizovaný systém správy a ověřování identit. V rámci návrhu řešení a údržby IS DMVS bude Zhotovitel aplikovat požadavky § 19 VoKB a požadavky Objednatele. Podrobný popis je uveden v kapitolách Autentizační modul a Registr Identit. Tento systém zajistí zejména:

- Ověření identity před zahájením aktivit v informačním a komunikačním systému,
- řízení počtu možných neúspěšných pokusů o přihlášení,
- odolnost uložených nebo přenášených autentizačních údajů proti neoprávněnému odcizení a zneužití,
- ukládání autentizačních údajů ve formě odolné proti offline útokům,
- opětovné ověření identity po určené době nečinnosti,
- dodržení důvěrnosti autentizačních údajů při obnově přístupu,
- centralizovanou správu identit.

Při implementaci změny využijeme doporučení k implementaci, např:

http://docs.oasis-open.org/security/v2.0/saml-sec-consider-2.0-os.pdf ,

https://www.owasp.org/index.php/SAML_Security_Cheat_Sheet

1.5.6.17. Řízení přístupových oprávnění

Pro řízení přístupových oprávnění Zhotovitel v rámci návrhu řešení a údržby IS DMVS bude aplikovat požadavky § 20VoKB a požadavky Objednatele tak, aby bylo zajištěno centralizované řízení oprávnění pro přístup k jednotlivým aktivům informačního a komunikačního systému a pro čtení dat, zápis dat a změnu oprávnění. Podrobný popis je uveden v kapitole Autentizační modul a Registr Identit.

1.5.6.18. Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů

Zhotovitel aplikuje pro IS DMVS požadavky § 22 VoKB a požadavky Objednatele. Dále zohlední doporučení NÚKIB na minimální požadavky pro logy, které musí být zajištěny pro spolehlivou ex-post analýzu kybernetických bezpečnostních incidentů a které vychází z dokumentu NIST800-92. V rámci logů budou zaznamenávány bezpečnostní, auditní a potřebné provozní události důležitých aktiv IS DMVS s konfigurovatelnou dobou retence záznamů:

- Události podle § 22, odst. 2) písm. d) vyhlášky č. 82/2018 Sb.,
  - přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů,
  - činnosti provedených administrátory,
  - úspěšné i neúspěšné manipulace s účty, oprávněními a právy,
  - neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,
  - činnosti uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému
  - zahájení a ukončení činností technických aktiv,

- kritické i chybové hlášení technických aktiv a přístupy k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí.

A dále:

- Významné události aplikační logiky (změna stavu entity, provolání aplikační funkce, …)
- Monitorování změnových událostí dat (modifikace, smazání významných entit, …)
- Provozní události systému, ukládají se do logů, které jsou plně konfigurovatelné včetně způsobu ložení a úrovně logování
- Provozní monitoring systému

Logování i audit budou aplikovány i pro Projektovou kancelář Zhotovitele.

Popis logování systémů (umístění logů apod., systém sledování) bude obsažen v provozní a instalační dokumentaci.

1.5.6.19. Detekce kybernetických bezpečnostních událostí

Detekce kybernetických bezpečnostních událostí bude v rámci komunikační sítě zajištěna především pomocí bezpečnostních prvků, kterými disponuje Objednatel a bude zajišťovat:

- ověření a kontrolu přenášených dat v rámci komunikační sítě a mezi komunikačními sítěmi,
- ověření a kontrolu přenášených dat na perimetru komunikační sítě a
- blokování nežádoucí komunikace.

V návaznosti na ZoKB je nutné detekovat kybernetické bezpečnostní události přiměřeně s ohledem na důležitost aktiv v rámci:

- serverů,
- datových úložišť a výměnných datových nosičů,
- síťových aktivních prvků,
- obdobných aktiv.

Projekt IS DMVS bude nutné zapojit do procesů souvisejících s procesy kybernetických bezpečnostních událostí Objednatele.

1.5.6.20. Aplikační bezpečnost

Metodika Zhotovitele pro vývoj a dodávek informačních řešení ADM (Asseco Delivery Methodology) stanovuje procesy a techniky pro vývoj bezpečného systému. Členové týmu v technických rolích (vývojáři, testeři) jsou školeni (OWASP Top Ten, OWASP Secure Coding Practices, Principle of least privileges, Secure Defaults, Testování bezpečnosti). Používány jsou pouze schválené nástroje pro vývoj. Jsou požívány pouze schválené knihovny. Jsou využívána doporučení OWASP Top 10, Cheat Sheets a další (při integraci s NIA se jedná např. o doporučení dokumentu SAML2 Security Considerations, využita budou i doporučení normy A.14.1.3 normy ISO/IEC 27002). Je prováděna controla kódu (code review). Jsou prováděny testy bezpečnostních funkcí a mechanismů, zda fungují očekávaným způsobem a mají požadované vlastnosti. Jsou prováděny zátěžové testy a testy bezpečnosti. Podrobný popis je uveden v příloze smlouvy Příloha SML13 – Metodika vývoje, kapitola 2.1.12.11 Bezpečnostní analýza kódu.

1.5.6.21. Kryptografické prostředky

Pro ochranu aktiv informačního a komunikačního systému bude použito aktuálně odolných kryptografických algoritmů a kryptografických klíčů dle doporučení v oblasti kryptografických prostředků vydaných Národním úřadem pro kybernetickou a informační bezpečnost (NUKIB). V rámci této oblasti bude prosazováno bezpečné nakládání s kryptografickými prostředky a využito bude systému správy klíčů a certifikátů. V řešení IS DMVS budou použité pouze aktuálně bezpečné

kryptografické protokoly. Zhotovitel bude udržovat podrobnou dokumentaci popisující používání kryptografických prostředků (implementační a provozní dokumentace).

Zhotovitel sleduje vývoj v oblasti kryptografie, vyhledává informace o zranitelnostech v implementaci algoritmů, protokolů, informace o vydavatelích certifikátů, a opatření (aktuální např. Certificate Transparency). V případě identifikace zranitelností následně pracovníci bezpečnostních rolí připraví návrhy opatření a informují Objednatele.

Zhotovitel má praktické zkušenosti s implementací a použitím kvalifikovaných elektronických pečetí a kvalifikovaných časových razítek.

1.5.6.22. Zajišťování úrovně dostupnosti informací

Zhotovitel navrhne řešení IS DMVS tak, aby zajistil dostupnost informačního a komunikačního systému pro splnění cílů podle Strategie řízení kontinuity činností, odolnost informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům, které by mohly snížit jeho dostupnost a dostupnost důležitých technických aktiv informačního a komunikačního systému a redundanci aktiv nezbytných pro zajištění dostupnosti informačního a komunikačního systému.

1.6. Monitorování provozu

1.6.1. Obecné zásady

Minimálně v období 3 pracovních dnů následujících po instalaci změn IS DMVS do produkčního prostředí, případně až do vyřešení zjištěných problémů, bude Zhotovitel provádět monitorování provozu IS DMVS. Monitorovány musí být zejména části IS DMVS, 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 IS DMVS, bude Zhotovitel upozorňovat Objednatele bezodkladně.

1.6.2. Popis monitorování provozu IS DMVS

Po instalaci změn do produkčního prostředí bude Zhotovitel provádět monitorování provozu DMVS. Monitorovány budou zejména části DMVS, které byly v rámci dané verze modifikovány nebo mohou být úpravami ovlivněny.

Pro monitoring bude Zhotovitel využívat monitorovací nástroje Objednatele.

Průběžným monitorováním a laděním, při nasazení na před-produkčních prostředích, bude zabezpečeno hladké nasazení na produkčním prostředí.

Součástí dodávky bude popis provozního monitorování včetně sledovaných metrik a jejich mezí a úrovní pro výstrahy (alerty). Součástí nasazení změn do produkčního prostředí bude současně také úprava nebo rozšíření monitorovaných metrik v monitorovacích nástrojích Objednatele v souladu s dodaným popisem. Součástí konfigurace bude také nastavení odesílání výstrah (alertů) na service desk Zhotovitele.

1.6.2.1. Způsob zajištění poinstalačního monitoringu provozu DMVS

Zhotovitel zajistí nepřetržitý service desk, který v případě příjmu výstrahy (alertu) z monitorování zajistí její předání odpovědným řešitelům Zhotovitele. Výsledky monitorování bude mít k dispozici také

Objednatel v rámci svého přístupu k monitorovacím nástrojům včetně možnosti příjmu příslušných výstrah (alertů).

Pro případ problémů, které mohou ohrozit funkčnost DMVS bude Zhotovitel na problémy bezodkladně upozorňovat dohodnutým komunikačním kanálem odpovědné osoby Objednatele.

Zhotovitel bude mít během poinstalačního monitoringu provozu DMVS v rámci PÚ v pohotovostním režimu pracovníky Zhotovitele v rolích DB administrátor, Specialista Oracle DB, Specialista Oracle Middleware, Vývojář frontend, Vývojář DB, Specialista infrastruktury tak, aby byl schopen zajistit činnosti související se zajištěním poinstalačního monitoringu.

V případě, že Objednatel poskytne definovaným osobám Zhotovitele potřebné podklady, zavazuje se Zhotovitel provádět následující činnosti během zajišťování poinstalačního monitoringu provozu DMVS v rámci PÚ:

- Kontrola logů a výstupů po instalaci dodávky do produkčního prostředí
- Kontrola a monitoring provozních a výkonnostních parametrů
- Identifikace provozních anomálií
- Kontrola aplikačních a provozních logů
- Profylaktické činnosti

Po skončení třídenního monitorování provozu po instalaci změn do produkčního prostředí dodá Zhotovitel Objednateli souhrnnou zprávu o průběhu monitorování.

Zhotovitel navrhuje zřídit (v případě, že neexistuje) u Objednatele centrální sběr a vyhodnocování logů ze všech komponent řešení (OS, AS, DB nebo aplikace). Možnost fulltextového prohledávání logů značně zvýší efektivitu dohledání příčin problémů při instalacích stejně jako při jakýchkoli jiných mimořádných událostech.

1.7. Zajištění podpůrných a souvisejících činností s plněním VZ

Zajištěním všech podpůrných a souvisejících činností s plněním Smlouvy se rozumí zejména:

- podpora při instalaci změn (dodávek) IS DMVS na referenční a produkční prostředí,
- vedení a administrace projektu,
- zajištění online dostupného zabezpečeného úložiště (viz čl. 11.8 Smlouvy)
- zřízení, zdokumentování a vedení projektové kanceláře (viz čl. 11.9 Smlouvy),
- zajištění a zdokumentování propojení HD systémů pro řízení testování (viz čl. 11.10 Smlouvy),
- komunikace s Objednatelem, účast na schůzkách, součinnost s třetími stranami.

Objednatel v této souvislosti požaduje, aby Zhotovitel v předstihu minimálně 5 dní před fakturací za PÚ předkládal Objednateli k odsouhlasení výkazy či přehledy s výsledky průběžné provozní údržby za dané období.