Příloha č. 6 - Bezpečnostní pravidla pro dodavatele VIS

Cílem těchto bezpečnostních pravidel je snižování kybernetických rizik a zvyšování účinnosti bezpečnostních opatření chránící Aktiva Krajského úřadu Jihomoravského kraje (dále jen „**KrÚ JMK**“), ke kterým mají přístup Dodavatelé dle ustanovení § 4 odst. 4 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění (dále jen „**Zákon**“), ve spojení v přílohou č. 7 k vyhlášce č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) (dále jen „**Vyhláška**“).

A.1 Základní odpovědnosti Dodavatele

Dodavatel řešení:

a. Je povinen postupovat v souladu s platnými a účinnými právními předpisy, zejména pak v souladu s požadavky vyplývajícími pro KrÚ JMK, jakožto správce a provozovatele Významného informačního systému, ze Zákona a Vyhlášky a reflektovat případné novely uvedených právních předpisů či novou právní úpravu;

b. Odpovídá za své řešení/dodávku/správu tak, aby respektovalo požadavky na bezpečnost KrÚ JMK, zabránilo bezpečnostním incidentům a krizovým situacím;

c. Odpovídá za dodávku a implementaci řešení v požadované kvalitě i z pohledu bezpečnosti.

d. Je povinen zajistit, aby předmět plnění nebyl nevyhovující z hlediska informační bezpečnosti, přičemž za nevyhovující je považováno jakékoli plnění, které obsahuje technologie/klíčové prvky, vůči jejichž výrobcům příslušný správní orgán vydal opatření v souladu se Zákonem, a které dle analýzy rizik představují vysoké riziko;

e. Je povinen provádět analýzu a hodnocení rizik informační infrastruktury, která je součástí předmětu Smlouvy (dodávaného řešení) a na základě výsledků navrhovat a předkládat KrÚ JMK ke schválení opatření na minimalizaci nebo odstranění zjištěných rizik;

f. Je povinen zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost během poskytování plnění pro KrÚ JMK;

g. Odpovídá za trvalé zachování mlčenlivosti všech svých pracovníků i po ukončení smluvního vztahu s KrÚ JMK.

A.2 Ochrana Aktiv

1. Dodavatel se před vlastním **přístupem** k datům a informacím KrÚ JMK musí zavázat mlčenlivostí. Tzn., že platí povinnost Dodavatele se zavázat a také povinnost pracovníků KrÚ JMK zavázat Dodavatele a nezpřístupnit data a informace Dodavateli dříve, než dojde k jeho závazku mlčenlivosti (tj. podpisu NDA – Non Disclosure Agreement či CA – Confidentiality Agreement).

A.3 Řízení přístupu k ICT/IS

1. Přihlášení Dodavatele do sítě KrÚ JMK musí podléhat kontrole přístupu na základě autorizace po předchozí autentizaci.

2. Dodavatel se zavazuje, že před připojením koncového zařízení, mobilní koncového zařízení nebo aktivního síťového prvku jako síťové switche, WiFi access pointy, routery či huby do počítačové sítě zažádá o schválení připojení kontaktní osobu na straně KrÚ JMK.
3. Dodavatel se zavazuje, že vzdálený přístup do systému KrÚ JMK bude vždy uskutečněn pouze prostřednictvím zabezpečeného připojení VPN.
4. Dodavatel se zavazuje, že bez zbytečného odkladu deaktivuje všechny nevyužívané zakončení sítě anebo nepoužívané porty aktivního síťového prvku.
5. Dodavatel se zavazuje, že nebude instalovat a používat zejména typy nástrojů Keylogger, Sniffer, Analyzátor zranitelností a Port Scanner, Backdoor, rootkit a trojský kůň nebo jinou podobu malware.
6. Dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění KrÚ JMK, které přistupují do interní sítě nebo informačního systému KrÚ JMK, měly v externím zařízení typu notebook/počítač aplikovány bezpečnostní záplaty a nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu.
7. Dodavatel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci Dodavatele nebo Poddodavatele.

A.4 Audit dodavatele

1. Dodavatel se zavazuje poskytnout KrÚ JMK veškeré informace potřebné k doložení toho, že byly splněny povinnosti vyplývající z těchto pravidel, jakož i ze Zákona a Vyhlášky, a za tímto účelem se zavazuje umožnit KrÚ JMK provedení kontrol, včetně auditů prováděných KrÚ JMK či auditorem, kterého KrÚ JMK k auditu pověří, a poskytne k těmto kontrolám a auditům veškerou potřebnou součinnost.
2. Dodavatel je povinen KrÚ JMK zpřístupnit veškerou potřebnou dokumentaci pro účely kontroly či auditu, zejména výčet technických a organizačních opatření.
3. Dodavatel má povinnost určit svého zástupce (případně své zástupce), který bude po dobu provádění kontroly či auditu přítomen.
4. Dodavatel je dále povinen umožnit provedení kontroly či auditu i ze strany dozorových orgánů.

A.5 Poddodavatelé

1. Dodavatel nezapojí do poskytování plnění dle této Smlouvy žádného dalšího Poddodavatele bez předchozího konkrétního nebo obecného povolení KrÚ JMK.
2. Dodavatel je povinen předat KrÚ JMK kontaktní údaje všech osob dodávajících systémovou a technickou podporu pro řešení.
3. Dodavatel má povinnost zajistit, že Poddodavatel bude v souladu s požadavky, které KrÚ JMK ukládá na základě těchto Bezpečnostních pravidel Dodavateli.
4. Dodavatel odpovídá za to, že jeho Poddodavatelé nebudou jednat v rozporu s bezpečnostními opatřeními vyplývajícími z těchto Bezpečnostních pravidel; v případě, že dojde k nedodržení těchto požadavků ze strany Poddodavatele Dodavatele, považuje se každé takové nedodržení požadavků za porušení povinnosti Dodavatele dle Smlouvy.

A.6 Řízení změn

1. KrÚ JMK v rámci řízení změn v systému řízení kybernetické bezpečnosti přezkoumává možné dopady změn a určuje významné změny dle Vyhlášky.
2. Dodavatel se zavazuje poskytnout KrÚ JMK veškerou nezbytnou součinnost při analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených

se změnami, aktualizaci bezpečnostní dokumentace, souvisejícím testováním a zajištění možnosti navrácení do původního stavu.

3. V případě realizace penetračního testování nebo testování zranitelnosti řešení poskytne Dodavatel KrÚ JMK veškerou potřebnou součinnost. Dodavatel je povinen přijmout dodatečná, účinná nápravná opatření k odstranění zranitelností, které byly zjištěny v průběhu penetračního testování.

A.7 Řízení bezpečnostních rizik

1. Dodavatel je povinen pravidelně provádět také vlastní hodnocení rizik a kontrolu zavedených bezpečnostních opatření. Tato kontrola probíhá v pravidelných intervalech stanovených Dodavatelem, na žádost KrÚ JMK. O výsledku kontroly podá Dodavatel KrÚ JMK bez zbytečného odkladu písemnou kontrolní zprávu.

A.8 Monitorování činností

1. Dodavatel bere na vědomí, že veškerá jeho aktivita realizovaná v informačních systémech, může být KrÚ JMK průběžně a pravidelně monitorována.
2. Předmět plnění musí poskytovat auditní záznamy (logy) o činnostech v něm provedených, v rozsahu stanoveném Vyhláškou, které umožní jednoznačně určit uživatele, čas a provedenu činnost.
3. Dodavatel se zavazuje, že umožní přístup k auditním údajům (systémové a aplikační logy) v takové podobě a formátu, který je možné dále zpracovávat v rámci systému Arcsight ESM z kategorie nástrojů SIEM (Security Information Event Management) a jejich archivaci pomocí nástroje Syslog-ng Store Box.

A.9 Zvládání kybernetických bezpečnostních incidentů

1. Dodavatel se zavazuje, že bude hlásit všechny nestandardní situace, bezpečnostní slabiny, kybernetické bezpečnostní události a incidenty včetně případů porušení zabezpečení osobních údajů neprodleně po jejich detekci KrÚ JMK.
2. Hlášení provádí Dodavatel telefonicky na linku + 420 541 658 903 a písemně na koc.incident@kr-jihomoravsky.cz. Součástí oznámení musí být popis povahy případu.
3. Pokud dojde ke kybernetické bezpečnostní události nebo ke kybernetickému bezpečnostnímu incidentu a následnému zvládání a vyhodnocování kybernetického bezpečnostního incidentu na bezpečnostní incident na straně KrÚ JMK, poskytne Dodavatel požadovanou součinnost např.: poskytne logy a identifikační údaje (např. IP adresa, MAC adresa, HW typ, sériové číslo případně IMEI) dotyčného koncového zařízení nebo mobilního koncového zařízení, k analýze obsahu, případně bez zbytečného odkladu zrealizuje opatření požadovaná KrÚ JMK).
4. Dodavatel má povinnost provést analýzu příčin kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování v případě, že Dodavatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

A.10 Informační povinnost dodavatele

1. Dodavatel má povinnost bez zbytečného odkladu informovat KrÚ JMK o významné změně ovládání Dodavatele podle zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích) nebo změně vlastnictví základních aktiv, jakož i změně v oprávnění Dodavatele nakládat s aktivy, které jsou využívány k plnění předmětu Smlouvy.

2. Dodavatel má povinnost informovat KrÚ JMK o způsobu řízení rizik, jakož i o zbytkových rizicích souvisejících s plněním předmětu Smlouvy.

A.11 Výměna informací

1. Dodavatel se zavazuje, že veškerý přenos dat a informací musí být dostatečně zabezpečen pomocí aktuálně odolných kryptografických algoritmů a kryptografických klíčů.
2. Dodavatel se zavazuje, že on-line transakce realizované prostřednictvím webových technologií budou chráněny SSL certifikáty.

A.12 Řízení kontinuity činností

1. KrÚ JMK má oprávnění zapojit Dodavatele do řízení kontinuity činností, a to zejména oprávnění k zahrnutí Dodavatele do plánu kontinuity činností, který souvisí s VIS a souvisejících služeb a/nebo zahrnutí Dodavatele do havarijního plánu KrÚ JMK.
2. Dodavatel předloží KrÚ JMK metodiku zálohování a obnovy dat ve formě zálohovacího plánu, testovacího scénáře obnovy dat, systému evidence, zajištění integrity a autenticity zálohovacího média. Záloha jako taková musí být šifrována.

A.13 Likvidace dat

1. Pokud v rámci plnění předmětu Smlouvy má Dodavatel povinnost k mazání dat a k likvidaci technických nosičů a/nebo provozních údajů a/nebo informací a jejich kopií, postupuje vždy v souladu s pravidly pro mazání dat a v souladu se způsoby likvidace technických nosičů informace, provozních údajů, informací a jejich kopií na základě tabulky č.1. Přičemž, pokud není určena klasifikace informace, bude použit způsob likvidace pro důležitost aktiva kritickou.

A.14 Povinnosti při ukončení smlouvy

1. Dodavatel se zavazuje poskytnout KrÚ JMK veškerou potřebnou součinnost, dokumentaci a informace, účastnit se jednání s KrÚ JMK a popřípadě třetími osobami za účelem plynulého a řádného převedení všech činností spojených s provozem, podporou a rozvojem předmětu Smlouvy na KrÚ JMK a/nebo nového dodavatele, ke kterému dojde po skončení účinnosti této Smlouvy, a to vše dle pokynů KrÚ JMK (dále jen „**Ukončení smlouvy**“).
2. Dodavatel se zavazuje za tímto účelem vypracovat a nejpozději spolu s provozní dokumentací ke každému předávanému dílčímu plnění předat KrÚ JMK dokumentaci, která bude stanovovat postup při Ukončení smlouvy (dále jen „**Plán**“). Dodavatel se zavazuje Plán po dobu trvání této Smlouvy průběžně aktualizovat a KrÚ JMK vždy při změně jakékoliv skutečnosti uvedené v Plánu předat aktualizovanou verzi Plánu zohledňující tuto změnu.
3. Dodavatel je povinen poskytnout plnění nezbytná k realizaci tohoto Plánu za přiměřeného použití vhodných ustanovení Smlouvy.
4. Strany se dohodly, že cena za vypracování Plánu a poskytnutí plnění nezbytného k realizaci Plánu je součástí ceny dle této Smlouvy.

Tato Bezpečnostní pravidla jsou v souladu s platnými právními předpisy České republiky. Pokud se jakékoli ustanovení těchto Bezpečnostních pravidel stane neplatným či nevymahatelným, nebude to mít vliv na platnost a vymahatelnost ostatních ustanovení těchto Bezpečnostních pravidel a rovněž

Smlouvy. Strany se zavazují nahradit neplatné nebo nevymahatelné ustanovení novým ustanovením, jehož znění bude odpovídat úmyslu vyjádřenému původním ustanovením a těchto Bezpečnostních pravidel jako celkem.

Tabulka č. 1

<table>
<tr><th></th><th colspan="4">Přípustný způsob likvidace podle úrovně důležitosti aktiva</th></tr>
<tr><th>Nosič informace</th><th>1. Nízká</th><th>2. Střední</th><th>3. Vysoká</th><th>4. Kritická</th></tr>
<tr><td>Informace na lidsky čitelném nosiči (tištěné dokumenty, poznámky a podobně)</td><td>Odstranění: Vyhození do odpadu.</td><td>Přepsání: Začernění.
Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje.</td><td colspan="2">Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje s podélným i příčným řezem, spálením nebo rozložením.</td></tr>
<tr><td>Mobilní zařízení (mobilní telefony, tablety)</td><td>Odstranění: Vymazání informací, reset zařízení do továrního nastavení.</td><td>Přepsání: Pro zařízení s šifrovaným úložištěm - odstranění informací a reset do továrního nastavení.</td><td colspan="2" rowspan="4">Fyzická likvidace: Rozebrání zařízení a zničení nosiče informací.</td></tr>
<tr><td>Síťová zařízení (router, switch, modem a podobně)</td><td rowspan="2">Odstranění: Vymazání informací, reset do továrního nastavení.</td><td rowspan="2">Přepsání: Odstranění a zahlcení umělými událostmi (umělý síťový provoz, testovací tiskové úlohy a podobně.).</td></tr>
<tr><td>Kancelářské vybavení (scanery, tiskárny, fax)</td></tr>
<tr><td>Magnetická média (magnetické pásky, disky, HDD [Hard Disk Drive])</td><td rowspan="3">Odstranění: Smazání dat na úrovni souborového systému.</td><td rowspan="2">Přepsání: Přepsání dat. V případě šifrovaného média je alternativou bezpečná likvidace kryptografických klíčů</td></tr>
<tr><td>Optická média (CD, DVD, HD-DVD, BLU-RAY)</td><td colspan="2" rowspan="2">Fyzická likvidace: Zničení nosiče informací.</td></tr>
<tr><td>Elektronická média (flash paměti)</td><td>Fyzická likvidace.</td></tr>
<tr><td rowspan="2">Outsourcing a cloud</td><td colspan="4">Přípustný způsob likvidace dat by měl být stanoven smluvním ujednáním.</td></tr>
<tr><td>Odstranění: Odstranění všech souborů včetně předchozích verzí.</td><td>Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná</td><td>Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace</td><td>Přepsání/fyzická likvidace: Použit způsob viz úroveň “3. Vysoká” nebo použita dedikovaná paměťová kapacita úložiště. Při</td></tr>
</table>

		likvidace kryptografických klíčů. Alternativně v případě dedikovaného paměťového média je možné data po ukončení služby přepsat.	kryptografických klíčů uložených v certifikovaném hardware security modulu (HSM) řízená zákazníkem (například podle standardu FIPS 140-2 Level 2). Při ukončení služby bude zlikvidován vrchní přístupový klíč a data jsou přepsána.	ukončení služby provedena celková sanitizace všech použitých paměťových médií podle výše uvedených řádků pro úroveň kritická.

1. SLUŽBY PODPORY A SLUŽBY ROZVOJE IS DTM JMK

1.1. Úvod

V rámci poskytování Služeb podpory a Služeb rozvoje objednatel získává nárok na to, že IS DTM a jeho funkcionality budou uvedeny v soulad s aktuálním stavem právního řádu v ČR (tj. v soulad s platnými obecně závaznými právními předpisy ČR a EU platnými a účinnými na území ČR), a to nejpozději ke dni, kdy nabyla nová právní úprava účinnosti. Implementace bude provedena v termínech navržených poskytovatelem po odsouhlasení objednatelem, nejpozději však k datu nabytí účinnosti nové právní úpravy. Pokud je implementace nové právní úpravy odvislá od vydání příslušných prováděcích předpisů zavazuje se poskytovatel provést instalaci a implementaci legislativního update v co nejkratším termínu. Nedojde-li k implementaci nejpozději do 60 kalendářních dnů od vydání příslušných prováděcích předpisů k právní úpravě, je Poskytovatel povinen Objednateli zdůvodnit, že k implementaci legislativního updatu došlo v co nejkratším termínu. Nebude-li Objednatel odůvodnění považovat za dostatečné, platí, že implementace legislativního updatu byla realizována opožděně.

1.2. Služby podpory

Služby podpory zahrnují služby technické podpory, správy a údržby IS DTM potřebné pro provoz IS DTM, tj. pro zajištění dostupnosti a správnosti všech funkcionalit IS DTM. Plnění Služeb podpory zahrnuje zejména:

- služby údržby IS DTM, tj. odstraňování vad a aktualizace SW produktů (poskytování a implementaci oprav a nových verzí SW produktů), a též opravy dat, pokud chyba dat nastala v důsledku vady IS DTM;
- služby správy IS DTM, tj. vykonávání pravidelných a proaktivních činností;
- služby technické podpory, tj. analýzu a řešení provozních incidentů v souladu se SLA parametry, analýzu a řešení problémů a rizik, řešení provozních požadavků Objednatele, poskytování součinností pro provozní činnosti Objednatele, zajištění školení při změnách IS DTM;
- řízení provozních procesů ve spolupráci s Objednatelem.

Poskytovatel je povinen poskytovat Služby podpory v souladu se Smlouvou a jejími přílohami a dále dle popisu, který je součástí Provozní dokumentace ve smyslu odst. 9.1 Technické specifikace, která tvoří přílohu č. 1 Smlouvy.

Vznikne-li při poskytování Služeb rozvoje Poskytovatelem výstup, k němuž bude možné a účelné poskytovat Služby podpory, zavazuje se Poskytovatel zahájit poskytování Služeb podpory rovněž k takovýmto výstupům ode dne jejich akceptace Objednatelem. Cena za poskytování služeb dle tohoto bodu Smlouvy je již zahrnuta v ceně za Služby podpory.

Řízení provozu IS DTM a Služeb podpory Poskytovatele bude probíhat na základě organizační struktury a postupů specifikovaných v Provozní dokumentaci, kde budou stanovena detailní pravidla řízení provozu, včetně detailního popisu provozních procesů. Provozní dokumentace bude zpracována na základě požadavků a informací uvedených ve Smlouvě a jejích přílohách, v souladu s požadovanými

provozními a bezpečnostními normami (zejména ČSN ISO/IEC 20000 a ČSN ISO/IEC 27000) a na základě konkrétního technického řešení IS DTM navrženého Poskytovatelem.

Poskytovatel je odpovědný za dostupnost a správnost všech funkcionalit IS DTM v rozsahu dle Smlouvy a dokumentace systému.

Odpovědností Poskytovatele je řešení vad IS DTM identifikovaných v průběhu provozu. Vadou je rozuměn stav IS DTM odlišný od Smlouvy, schválených návrhových dokumentů a schválené dokumentace systému. Řešení vad probíhá primárně v rámci procesu řízení incidentů. Řešení vad komplikovanějšího charakteru, které aktuálně neomezují chování systému, může po schválení Objednatelem probíhat rovněž v rámci procesu řízení problémů nebo procesu řízení rizik.

Řešení všech incidentů, požadavků, problémů, rizik a změn (včetně součinností v rámci odpovídajících procesů), které souvisí s prevencí výskytu, opravou nebo řešením následků vad Díla, aktualizací SW produktů a souvisejících úprav nebo migrací dat, souvisejících úprav dokumentace a školení, nebo jejichž příčina nebyla dosud jednoznačně určena mimo oblast odpovědnosti Poskytovatele, je součástí ceny Služeb podpory. Všechny pravidelné a proaktivní činnosti, které jsou nezbytné pro provoz IS DTM bez výskytu provozních incidentů v oblastech odpovědnosti Poskytovatele, jsou rovněž součástí ceny Služeb podpory.

Součástí ceny Služeb podpory je současně 20 MD ročně na součinnosti Poskytovatele při řešení ostatních incidentů, problémů, rizik a změn, pravidelných a proaktivních činností a požadavků vyžádaných Objednatelem. V případě, že tento počet MD nebude v příslušném roce provozu vyčerpán, je možno nevyčerpané MD převést do následujícího roku provozu.

Poskytovatel je povinen poskytovat Objednateli garantovanou pomoc při řešení technických problémů souvisejících s provozem aplikace. Jedná se o vzdálené konzultace a řešení po telefonu, emailu, příp. s využitím aplikace HelpDesk. Tato podpora je poskytována v pracovní dny vždy nepřetržitě od 08:00 do 16:00 hodin.

Řešení incidentů

Poskytovatel je odpovědný za řešení provozních incidentů. Provozním incidentem (nebo jen incidentem) se rozumí výskyt chování odlišného od dokumentace systému a/nebo Smlouvy, nebo které omezuje použití nebo dostupnost systému.

Poskytovatel je plně odpovědný za dostupnost IS DTM a řešení incidentů dle uvedených parametrů Service Level Agreements. Incidenty způsobené nefunkčností technické infrastruktury nebo některých jejích částí v odpovědnosti Objednatele nebo zásahem Objednatele do IS DTM jsou vyloučeny z odpovědnosti Poskytovatele. Rozhodnutí, zda incident spadá do odpovědnosti Poskytovatele, provede Objednatel na základě vyhodnocení postupu analýzy a řešení incidentu, případně na základě dalších předložených technických podkladů, v souladu s rozdělením odpovědnosti popsaným ve Smlouvě a jejích přílohách.

Podpora SW produktů, které jsou součástí IS DTM, je považována za součást podpory IS DTM a musí splňovat stejné SLA parametry.

V případě dopadu nefunkčnosti spolupracujících externích systémů na funkčnost IS DTM je výsledné omezení provozu vyloučeno z odpovědnosti Poskytovatele. Poskytovatel je nicméně povinen v rámci návrhu a implementace systému definovat a implementovat mechanismy, které minimalizují vliv nefunkčnosti spolupracujících externích systémů na funkčnost IS DTM (např. ošetření chybových stavů, opakování neúspěšných operací, využití nakešovaných informací – v případech, kde je to možné a umožní alespoň částečnou funkci systému) a dále je povinen v průběhu poskytování Služeb podpory tyto mechanismy dále rozvíjet a upravovat na základě provozních zkušeností.

Ve všech výše uvedených případech je Poskytovatel spoluzodpovědný za řešení incidentů následujícími způsoby: včasný záznam postupu řešení v Service Desk Poskytovatele (dále jako „SD“), spolupráce na analýze incidentů, a v případě požadavku schváleného Objednatelem spolupráce na řešení nebo příprava dočasného náhradního řešení (work-around). Dokud není jednoznačně určená příčina incidentu mimo oblast odpovědnosti Poskytovatele, analyzuje a řeší Poskytovatel incident jako vlastní incident v souladu se SLA parametry. SD musí umožnit zadat Objednateli incident, min. kat. A, v režimu 7 x 24.

Klasifikace incidentů

Každý incident je vyhodnocován v kontextu všech základních částí, jejichž funkcionalitu ovlivňuje.

a) Incident kategorie A (výpadek)

IS DTM není použitelný ve svých základních a klíčových funkcích nebo není dostupný většině uživatelů. Tento stav kritickým způsobem ohrožuje klíčové odpovědnosti, procesy a aktivity Objednatele, případně způsobuje větší finanční nebo jiné kritické škody.

b) Incident kategorie B

IS DTM je ve své funkcionalitě omezen tak, že tento stav významně omezuje běžné použití IS DTM ze strany uživatelů.

c) Incident kategorie C

Drobné incidenty, které neomezují základní funkčnost a neomezují významně běžné použití IS DTM uživateli nebo způsobují omezení, které lze uživatelsky řešit jiným způsobem.

Definice SLA parametrů

A) Provozní doba je definována jako časové období, kdy musí být funkcionalita IS DTM dostupná a funkční a vůči které se vztahují ostatní SLA parametry. Schválené plánované odstávky nejsou výjimkou z provozní doby. Plánované odstávky podléhají schvalování Objednatele.

B) Dostupnost je poměrná část roku (viz odst. 7.3 technické specifikace, která tvoří přílohu č. 1 Smlouvy), kdy není aktivní žádný nevyřešený incident kategorie A (výpadek). Parametr dostupnosti je vyhodnocován na roční bázi, počínaje okamžikem zahájení poskytování Služeb podpory.

C) Doba odezvy je definována jako doba v provozní době mezi oznámením incidentu Poskytovateli a informováním Objednatele o krocích vedoucích k jeho řešení a v případě možnosti také o předpokládané době jeho ukončení.

D) Doba vyřešení je definována jako doba v provozní době mezi oznámením incidentu Poskytovateli a jeho vyřešením a obnovením funkcionality.

E) Počet incidentů dané kategorie za měsíc je počítán pro každý kalendářní měsíc podle času vzniku incidentu.

Hodnoty SLA parametrů

Při řešení provozních incidentů je Poskytovatel povinen dodržet lhůty stanovené v této kapitole. Poskytovatel je odpovědný za škody způsobené nedodržením SLA parametrů. Veškeré SLA parametry uvedené ve Smlouvě a jejích přílohách se týkají pouze produkčního prostředí.

Incident kategorie A

Doba odezvy (provozní doba v pracovní dny v rozmezí 7:00 – 17:00): 2 hodiny

Doba vyřešení (provozní doba v pracovní dny v rozmezí 7:00 – 17:00): 24 hodin

Maximální počet incidentů za kalendářní rok: 3

Incident kategorie B

Doba odezvy (provozní doba v pracovní dny v rozmezí 7:00 – 17:00): 4 hodiny

Doba vyřešení (provozní doba v pracovní dny v rozmezí 7:00 – 17:00): 48 hodin

Maximální počet incidentů za kalendářní měsíc: 1

Incident kategorie C

Doba odezvy (provozní doba v pracovní dny v rozmezí 7:00 – 17:00): 16 hodin

Doba vyřešení (provozní doba v pracovní dny v rozmezí 7:00 – 17:00): 96 hodin

Maximální počet incidentů za kalendářní měsíc: 5

Pro vyloučení pochybností je uveden modelový příklad výpočtu SLA:

K výpadku dojde v sobotu v 18:00. Lhůta pro odezvu i odstranění začne běžet v pondělí v 7:00. Pokud dojde k odezvě v pondělí v 8:00 a k odstranění lhůty ve středu v 11:00, pak by SLA byla počítána takto:

- Doba odezvy: 1 hodina - splněno
- Doba vyřešení: 10 hodin za pondělí + 10 hodin za úterý + 4 hodiny za středu = 24 hodin – splněno
- Doba nedostupnosti: 6 hodin za sobotu + 24 hodin za neděli + 24 hodin za pondělí + 24 hodin za úterý + 11 hodin za středu = 89 hodin – vyhodnocení by proběhlo po skončení kalendářního roku

Řízení požadavků

Poskytovatel bude dále vykonávat provozní požadavky vyžádané Objednatelem, potřebné k zajištění provozu IS DTM. Provozní požadavky mohou být vyžádány i v oblastech pravidelných a proaktivních činností. Poskytovatel je povinen řešit požadavky v rámci provozní doby systému bez zbytečného odkladu s ohledem na důležitost požadavků, určenou Objednatelem.

Pravidelné a proaktivní činnosti

V rámci činností správy a údržby je Poskytovatel povinen vykonávat pravidelné a proaktivní činnosti potřebné k zajištění bezchybného provozu IS DTM a schválené Objednatelem. Rozsah pravidelných a proaktivních činností vyplývá z potřeb provozu IS DTM, tj. zajištění dostupnosti a správnosti všech funkcionalit a naplnění všech provozních a bezpečnostních procesů.

V rámci pravidelných a proaktivních činností je Poskytovatel odpovědný za kontroly a návrhy změn konfigurace, kontroly a analýzy logů, ladění a optimalizaci IS DTM, profylaxi a proaktivní údržbu potřebnou k předcházení incidentům a veškeré další administrátorské činnosti na aplikační úrovni potřebné pro provoz IS DTM.

Předmětem profylaxe budou zejména tyto činnosti:

- kontrola bezpečnosti, funkcionality a odezvy systému,
- kontrola zálohování a bezpečnosti dat,
- mapování vytížení systému a návrh optimalizace (zejména selekty a indexy),
- nahrávání opravných dávek.

Poskytovatel je povinen na základě analýzy incidentů navrhovat, a po schválení Objednatele na úrovni aplikace, SW produktů a dat implementovat nové metriky provozního a bezpečnostního monitoringu s cílem zrychlení detekce incidentů. Poskytovatel je dále povinen navrhovat a po schválení Objednatelem provádět aktualizace SW produktů s cílem udržení aktuálnosti a bezpečnosti IS DTM.

Řízení změn a konfigurací

a. Provozní změny

Provozní změny jsou změny systému, které nemají vliv na rozsah IS DTM nebo Služeb podpory dle Smlouvy včetně jejích příloh a schválené dokumentace, např. změny spojené s řešením vad, optimalizací systému, drobné rekonfigurace, správa uživatelů, úpravy monitoringu nebo aktualizace firmware zařízení nebo SW produktů. Provozní změny mohou nastat jako součást řešení incidentů, požadavků, problémů, ošetření rizik nebo pravidelných a proaktivních činností.

Řízením změn a konfigurací je rozuměn proces evidence provozních změn v SD (včetně procesu jejich schvalování) a v konfigurační databázi (CMDB). Všechny provozní změny musí být schváleny Objednatelem.

Podmínkou schválení změn je jejich otestování na testovacím prostředí. Pokud to není možné z technických nebo časových důvodů, rozhoduje o nasazení změny do produkčního prostředí Objednatel.

Poskytovatel je odpovědný za pravidelnou aktualizaci dokumentace IS DTM včetně promítnutí provedených provozních změn.

b. Ostatní změny

Řízení ostatních změn systému, které mají vliv na rozsah IS DTM, probíhá primárně formou Služeb rozvoje.

Řízení problémů

Problém je příčinou jednoho nebo více incidentů. Příčina problému obvykle není známa v čase vyřešení incidentu a hrozí opakování výskytu incidentu. Proces řízení problémů řídí další zkoumání a řešení problému, včetně vyhodnocení efektivity řešení. Cílem řízení problémů není případným problémům zabránit, ale řešit je. Každý problém je třeba včas identifikovat, navrhnout řešení a řešení schválit.

Problémy jsou průběžně identifikovány všemi účastníky provozu na základě analýzy incidentů. Odpovědnost za návrhy a implementaci řešení vychází z rozdělení odpovědností Poskytovatele a Objednatele. Řešení problému schvaluje Objednatel. Pokud řešení problému vyžaduje změnový požadavek nebo realizaci Služeb rozvoje, postupuje se podle pravidel řízení změn.

Poskytovatel je povinen řešit problémy v rámci provozní doby systému bez zbytečného odkladu, s ohledem na závažnost problému, určenou Objednatelem. Do určení příčiny problému řeší Poskytovatel problémy přidělené Objednatelem jako problémy v odpovědnosti Poskytovatele.

Stav řešení je sledován na úrovni vedení provozu a evidován v řídícím dokumentu s názvem „Registr otevřených otázek, problémů a změn“.

Řízení rizik

Proces řízení rizik zahrnuje identifikaci a vyhodnocení rizik, stanovení a implementace vhodných opatření a vyhodnocení jejich účinnosti.

Provozní rizika jsou průběžně identifikována všemi účastníky provozu. Odpovědnost za návrhy a implementaci opatření vychází z rozdělení odpovědností implementace a provozu popsaných ve Smlouvě a jejích přílohách. Opatření schvaluje Objednatel. Pokud implementace opatření vyžaduje změnový požadavek nebo realizaci Služeb rozvoje, postupuje se podle pravidel řízení změn.

V rámci identifikace rizik musí být určeny:

- příčina rizika (reálná událost nebo situace, která je důvodem vzniku rizika);
- riziko (událost, která může s určitou pravděpodobností nastat);
- dopad na kvalitu a parametry poskytované služby.

Hodnocení rizik probíhá z hledisek:

- pravděpodobnosti, že riziková situace nastane,
- rozsahu dopadu v případě, že riziková událost nastane,
- časového horizontu, ve kterém může daná riziková událost nastat.

Poskytovatel je povinen implementovat opatření v rámci provozní doby systému bez zbytečného odkladu, s ohledem na závažnost rizika, určenou Objednatelem.

Stav rizik a jejich opatření je sledován v rámci jednání a úkolů řídících struktur provozu na úrovni vedení projektu a evidován v řídícím dokumentu „Registr rizik“.

Řízení kvality

Řízení kvality provozu probíhá na úrovni v rámci jednání a úkolů řídících struktur provozu a prostřednictvím pravidelných čtvrtletních zpráv.

Řízení kvality probíhá zejména v oblastech:

- plnění SLA parametrů

- eskalace, sledování a reporting řešení závažných incidentů s velkým dopadem na uživatele
- plnění provozních procesů řízení incidentů a požadavků
- prováděné pravidelné a proaktivní činnosti
- plnění provozního procesu řízení změn a konfigurací
- plánování a řízení změn většího rozsahu, včetně testování a nasazení do produktivního provozu
- stav problémů
- stav rizik.

Struktura pravidelné měsíční zprávy bude obsahem Provozní dokumentace.

1.3. Služby rozvoje

Tato kapitola obsahuje základní pravidla objednávání, řízení a vypořádání Služeb rozvoje. Detailní metodika řízení Služeb rozvoje bude dále upřesněna v Provozní dokumentaci.

1.3.1. Objednávání Služeb rozvoje

a) Služby rozvoje jsou objednávány oprávněnou osobou Objednatele, která zašle oprávněné osobě Poskytovatele poptávku emailem nebo jiným písemným způsobem. Poptávka minimálně obsahuje:

   i) specifikaci požadované Služby rozvoje;

   ii) požadovaný termín realizace Služby rozvoje;

   iii) požadovaný termín předložení nabídky, který nesmí být kratší než 1 týden od doručení poptávky, nedohodnou-li se smluvní strany jinak.

b) Poskytovatel v požadovaném termínu předloží emailem nebo jiným písemným způsobem nabídku Služby rozvoje, která bude obsahovat:

   i) způsob řešení poptávky;

   ii) termín realizace Služby rozvoje;

   iii) předpokládanou kapacitní náročnost vyjádřenou v člověkodnech nebo jeho částech, případně potřebné doplňující licence;

   iv) maximální cenu služby vypočítanou jako součin kapacitní náročnosti a jednotkové ceny člověkodne pro Služby rozvoje;

   v) požadovanou součinnost Objednatele;

   vi) požadované změny v infrastrukturních požadavcích Poskytovatele;

   vii) rizika realizace Služby rozvoje a způsob jejich mitigace.

c) Objednatel je oprávněn požadovat po Poskytovateli upřesnění nebo doplnění nabídky Služby rozvoje, a to i opakovaně.

d) Souhlasí-li Objednatel s nabídkou Poskytovatele, předá Poskytovateli způsobem stanoveným v Řídicí dokumentaci provozu poptávkový formulář (dále jen „***Poptávkový formulář***“), který bude obsahovat:

i) specifikaci požadované Služby rozvoje;

ii) požadovaný termín realizace Služby rozvoje;

iii) kapacitní náročnost;

iv) maximální cenu;

v) specifikaci součinnosti Objednatele;

vi) aktualizaci infrastrukturních požadavků Poskytovatele;

vii) specifikaci případných ostatních povinností Poskytovatele.

e) Poskytovatel potvrdí přijetí Poptávkového formuláře do 2 pracovních dní způsobem stanoveným v Řídicí dokumentaci provozu.

1.3.2. Implementace Služeb rozvoje

Při implementaci Služeb rozvoje jsou dodržovány principy a požadavky realizace dodání IS DTM, zjednodušené v míře odpovídající řídícím strukturám provozu a rozsahu změn v rámci konkrétní služby rozvoje. Jedná se zejména o rozdělení odpovědností při implementaci a dále o oblasti vývoje, testování a dokumentace systému.

Při implementaci Služeb rozvoje jsou dodržovány provozní procesy platné pro Služby podpory, zejména řízení změn a konfigurací a řízení součinností.

Součástí Služeb rozvoje je i aktualizace dotčené dokumentace IS DTM.

1.3.3. Vypořádání Služeb rozvoje

Po splnění Služeb rozvoje je Poskytovatel povinen k Akceptačnímu protokolu připojit výkaz skutečně odpracovaných člověkodní nebo jejich částí a adekvátně stanovit finální cenu práce za Službu rozvoje, která nesmí překročit maximální cenu práce v Poptávkovém formuláři.