Technická a funkční specifikace provizorního ISMS

Vymezení věcné oblasti plnění

Obsah

1 Předmět plnění

IBM (dále jen „***IBM***“ nebo „***Zadavatel***“ nebo „***Objednatel***“) poptává službu Housing pro Provizorní zajištění majetkového a ekonomického modulu pro agendu ÚZSVM. Provizorní majetkový a ekonomický modul mají krátkodobě nahradit stávající Informační systém majetku státu (dále jen „***stávající ISMS***“), a to bez modulu Centrální registr administrativních budov, a to do doby, než bude nasazen nový systém ve vlastnictví ÚZSVM, který bude tuto agendu dlouhodobě zajišťovat (dále jen „***nový ISMS***“).

Služba Housing představuje služby bezpečného datového centra TIER III, které SPCSS poskytuje jednak jako samostatnou službu a též jako integrální součást dalších nadstavbových modelů služeb typu Hosting. V rámci služby Housing je Objednateli poskytována možnost umístění jeho ICT technologií, instalovaných do standardních racků, v bezpečném datovém centru (BDC). Z pohledu šíře služeb se jedná o zcela základní službu, kdy odpovědnost za ICT technologie umístěné v DC i za jejich podporu je plně na straně Objednatele.

Součástí služeb datového centra, resp. Housingu, je:

- zálohované napájení a chlazení technologií,
- příslušný provozní monitoring,
- zajištění fyzické a kybernetické bezpečnosti.

Provoz všech služeb bezpečného datového centra je procesně řízen a zahrnuje zejména následující procesy:

- management incidentů,
- management problémů,
- management kapacit,
- management požadavků,
- management úrovně služby vč. reportingu.

SPCSS jako Poskytovatel Služby zajistí formou pronájmu poskytnutí 2 uzamykatelných racků pro instalaci technických a telekomunikačních zařízení Zadavatele s 3 fázovým napájením v prostorách bezpečného datového centra (BDC) Poskytovatele. Specifikace pronajatého Racku a jeho garantovaný příkon je uveden v následující tabulce:

ID	Popis	Šíře racku	Garantovaný příkon pro každý jednotlivý rack
1	1 rack vč. prostoru v BDC	800 mm	6 kW

V prostorách Poskytovatele je možné umístit pouze telekomunikační zařízení, která nebudou narušovat provozní podmínky v BDC Poskytovatele a ovlivňovat ostatní zde umístěné technologie (například nelze v BDC umístit silné vysílače elektromagnetického vlnění, extrémně hlučná zařízení, zařízení ovlivňující extrémním způsobem teplotu, vlhkost nebo prašnost okolí).

Zadavatel odpovídá za provádění revizí a prohlídek vyhrazených technických zařízení, která jsou v jeho vlastnictví, v souladu s příslušnými právními předpisy a příslušnými ČSN. Služba bude zajištěna bez související kabeláže, s výjimkou zabezpečení kabelového propojení pro připojení k síti MV, tj. připojení do CMS2 (avšak bez konfiguračního nastavení a další správy připojení do CMS2).

Cena za Iniciaci Služby zahrnuje rovněž náklady na přípravu a zavedení služby, tj. součinnost Poskytovatele při instalaci technologií Zadavatele v datovém centru Poskytovatele. Součástí ceny

služby provozu je rovněž příslušný provozní dohled non IT technologií. Provádění dodatečných změn vyžádaných Zadavatelem není zahrnuto v měsíční ceně za poskytování služby. Cena Služeb je bez související kabeláže, s výjimkou kabelového propojení pro připojení k síti MV pro připojení do CMS2 (bez nastavení a další správy připojení do CMS2).

Pro relevantní typy služeb bude Dodavatel využívat "single point of contact" aplikaci typu Service Desk, kterou mu poskytne Zadavatel k dispozici.

Stávající ISMS je určen jako významný informační systém dle vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů. Vzhledem k tomu, že v provizorním ISMS budou zpracovávána stejná data, musí být v infrastrukturní rovině v souladu s požadavky na provoz významných informačních systémů dle právních předpisů.

1.1 Přehled relevantních předpisů

Provizorní ISMS musí poskytovat uživatelům na straně ÚZSVM kompletní softwarovou podporu pro svou činnost. Provizorní ISMS musí být v souladu s předpisy, které jsou uvedeny níže v tomto ustanovení. Dodavatel musí v rámci svého předmětu plnění zohlednit i veškeré související relevantní prováděcí předpisy.

- Zákon č. 110/2019 Sb., o zpracování osobních údajů
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů
- Zákon č. 111/2009 Sb., o základních registrech
- Zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů
- Zákon č. 171/2012 Sb., kterým se mění zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla), ve znění pozdějších předpisů
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů
- Zákon č. 183/2006 Sb., o územním plánování a stavebním řádu (stavební zákon), ve znění pozdějších předpisů
- Zákon č. 201/2002 Sb., o Úřadu pro zastupování státu ve věcech majetkových, ve znění pozdějších předpisů
- Zákon č. 202/2002 Sb., kterým se mění zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů, zákon č. 182/1993 Sb., o Ústavním soudu, ve znění pozdějších předpisů, zákon č. 89/1995 Sb., o státní statistické službě, ve znění pozdějších předpisů, zákon č. 77/1997 Sb., o státním podniku, ve znění pozdějších předpisů, zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla), ve znění pozdějších předpisů, zákon č. 65/1965 Sb., zákoník práce, ve znění pozdějších předpisů, a zákon č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích, ve znění pozdějších předpisů, ve znění pozdějších předpisů
- Zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla), ve znění pozdějších předpisů
- Zákon č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích, ve znění pozdějších předpisů
- Zákon č. 23/2017 Sb., o pravidlech rozpočtové odpovědnosti
- Zákon č. 25/2017 Sb., o sběru vybraných údajů pro účely monitorování a řízení veřejných financí, ve znění pozdějších předpisů
- Zákon č. 250/2017 Sb., o elektronické identifikaci
- Zákon č. 256/2013 Sb., o katastru nemovitostí (katastrální zákon), ve znění pozdějších předpisů
- Zákon č. 279/2003 Sb., o výkonu zajištění majetku a věcí v trestním řízení a o změně některých zákonů, ve znění pozdějších předpisů
- Zákon č. 290/2002 Sb., o přechodu některých dalších věcí, práv a závazků České republiky na kraje a obce, občanská sdružení působící v oblasti tělovýchovy a sportu a o souvisejících změnách a o změně zákona č. 157/2000 Sb., o přechodu některých věcí, práv a závazků z

majetku České republiky, ve znění zákona č. 10/2001 Sb., a zákona č. 20/1966 Sb., o péči o zdraví lidu, ve znění pozdějších předpisů, ve znění pozdějších předpisů

- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů
- Zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů
- Zákon č. 320/2002 Sb., o změně a zrušení některých zákonů v souvislosti s ukončením činnosti okresních úřadů, ve znění pozdějších předpisů
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů
- Zákon č. 412/2005 Sb., o ochraně utajovaných skutečností a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
- Zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů
- Zákon č. 59/2017 Sb., o použití peněžních prostředků z majetkových trestních sankcí uložených v trestním řízení a o změně některých zákonů, ve znění pozdějších předpisů
- Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
- Zákon č. 92/1991 Sb., o podmínkách převodu majetku státu na jiné osoby, ve znění pozdějších předpisů
- Vyhláška č. 133/2013 Sb., o stanovení rozsahu a struktury údajů pro vypracování návrhu zákona o státním rozpočtu a návrhu střednědobého výhledu státního rozpočtu a lhůtách pro jejich předkládání, ve znění pozdějších předpisů
- Vyhláška č. 220/2013 Sb., o požadavcích na schvalování účetních závěrek některých vybraných účetních jednotek, ve znění pozdějších předpisů
- Vyhláška č. 270/2010 Sb., o inventarizaci majetku a závazků, ve znění pozdějších předpisů
- Vyhláška č. 312/2014 Sb., o podmínkách sestavení účetních výkazů za Českou republiku (konsolidační vyhláška státu), ve znění pozdějších předpisů
- Vyhláška č. 323/2002 Sb. o rozpočtové skladbě, ve znění pozdějších předpisů
- Vyhláška č. 383/2009 Sb., o účetních záznamech v technické formě vybraných účetních jednotek a jejich předávání do centrálního systému účetních informací státu a o požadavcích na technické a smíšené formy účetních záznamů (technická vyhláška o účetních záznamech), ve znění pozdějších předpisů
- Vyhláška č. 410/2009 Sb., kterou se provádějí některá ustanovení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, pro některé vybrané účetní jednotky, ve znění pozdějších předpisů
- Vyhláška č. 416/2004 Sb., kterou se provádí zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění zákona č. 309/2002 Sb., zákona č. 320/2002 Sb. a zákona č. 123/2003 Sb., ve znění pozdějších předpisů
- Vyhláška č. 5/2014 Sb., o způsobu, termínech a rozsahu údajů předkládaných pro hodnocení plnění státního rozpočtu, rozpočtů státních fondů, rozpočtů územních samosprávných celků, rozpočtů dobrovolných svazků obcí a rozpočtů Regionálních rad regionů soudržnosti, ve znění pozdějších předpisů
- Vyhláška č. 62/2001 Sb., o hospodaření organizačních složek státu a státních organizací s majetkem státu, ve znění pozdějších předpisů
- Vyhláška 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), ve znění pozdějších předpisů
- Nařízení vlády č. 351/2013 Sb., kterým se určuje výše úroků z prodlení a nákladů spojených s uplatněním pohledávky, určuje odměna likvidátora, likvidačního správce a člena orgánu právnické osoby jmenovaného soudem a upravují některé otázky Obchodního věstníku, veřejných rejstříků právnických a fyzických osob a evidence svěřeneckých fondů a evidence údajů o skutečných majitelích, ve znění pozdějších předpisů
- Nařízení vlády č. 41/2017 Sb., o údajích centrálního registru administrativních budov
- Nařízení Evropského parlamentu a Rady (EU) 2016/679, nové obecné nařízení Evropské unie (EU) o ochraně osobních údajů a o volném pohybu těchto údajů
- České účetní standardy
- Metodika křížových kontrol – PAP a PKP

2 Technické a nefunkční požadavky

2.1 Bezpečnost systému

Dodavatel musí v rámci svého předmětu plnění podporovat požadavky uvedené v tomto článku. Systém musí naplňovat veškeré bezpečnostní požadavky dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a navazující vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti jako významný informační systém.

Systém řízení bezpečnosti musí být navržen a implementován v souladu s normami řady ISO/IEC 270xx (včetně rozšiřující normy ISO 27552), ISO 29151, ISO 29100:2011, a systém řízení provozu a správy provizorního ISMS musí být navržen a implementován v souladu s normou ČSN ISO/IEC 20000.

Systém bude ve výchozím stavu v souladu s bezpečnostním přístupem "Co není povoleno, je zakázáno". Tedy, pokud správce nenastaví uživateli práva, nebude mít uživatel přístup v systému k žádné akci, ani k žádným datům.

Systém bude vyhodnocovat práva k jednotlivým objektům a metodám systému na rozhraní aplikačního serveru tak, aby při obejití prezentační vrstvy běžící na klientské stanici nedošlo k prolomení bezpečnosti systému. Bezpečnost metod rozhraní aplikačního serveru bude ověřena bezpečnostními testy.

Pokud bude systém podporovat klienta nebo jiné rozhraní pro uživatele na mobilních platformách bez zabezpečení VPN, musí být způsob zabezpečení dat na těchto platformách v souladu s interními předpisy správce a provozovatele systému a platnou legislativou (např. splnění podmínek bezpečnostní dokumentace ohledně BYOD, BYOC nebo GDPR).

Součástí údajů vedených v provizorním ISMS budou údaje klasifikované dle zákona č. 110/2019 Sb., o zpracování osobních údajů jako osobní údaje a dále údaje, se kterými musí být nakládáno v souladu s GDPR.

V rámci dodávky provizorního ISMS je požadována součinnost Dodavatele se Zadavatelem při zpracování typového bezpečnostního projektu v souladu s uznávanými pravidly a normami, vytvořený pro konkrétní navržené technické řešení.

V rámci bezpečnostního projektu Dodavatel vypracuje minimálně následující:

- zohlednění požadavků řízení rizik bezpečnosti informací dle ISO 27005;
- doporučená bezpečnostní opatření;
- scénář pro pravidelné prověřování účinnosti bezpečnostních opatření a jejich dodržování;
- scénář pro testy zranitelnosti.

Výstupem bezpečnostního projektu, zpracovaného v rámci dodávky plnění, bude bezpečnostní dokumentace systému.

Provizorní ISMS musí být odolný proti známým bezpečnostním hrozbám a útokům z vnějších i vnitřních sítí. Webové části provizorního ISMS musí být chráněny proti známým útokům, které byly identifikovány nezávislým společenstvím OWASP (www.owasp.org). Systém a jeho dokumentace musí vyhovovat požadavkům právní úpravy dle GDPR a eIDAS a na ně navazující vnitrostátní úpravy.

Dodavatel musí mít a při poskytování služeb využívat formalizovanou metodiku pro vývoj, programování a kódování aplikace zahrnující i požadavky na bezpečnost, včetně opatření na ochranu proti škodlivým kódům. Metodika bude též zahrnovat základní principy organizační bezpečnosti pro vývoj a testování aplikace.

2.2 Dostupnost systému a Provozní doba

Je požadován režimu dostupnosti „7x24" s povolenými plánovanými servisními odstávkami uvedenými v odst. 2.4. V době mimo plánované servisní odstávky je požadována dostupnost:

- 98,8 % měsíčně - maximální celková přípustná doba nedostupnosti za kalendářní měsíc činí 9 hodin.

Provozní doba systému je požadována v pracovní dny mezi 8:00 až 17:00. Provozní doba je definována jako doba v dostupnosti systému, ve které musí být zajištěny všechny služby související s provozem systému a nesmí být plánovány žádné servisní odstávky.

2.3 Měření dostupnosti a vyhodnocení služby

V průběhu poskytování služeb dodávky systému je Zadavatel oprávněn po předchozím oznámení ověřit formou auditu (vlastními pracovníky nebo jím pověřenou třetí stranou) parametry požadované služby. To se týká rovněž dalších oprávněných osob, pokud toto jejich oprávnění vyplývá z právních předpisů.

Dodavatel je v takovém případě povinen poskytnout pověřeným pracovníkům Zadavatele či pověřené třetí straně součinnost, umožnit přístup do prostor Dodavatele a na vyžádání poskytovat ústní či písemná vyjádření.

Vyhodnocení služby

Dodavatel bude prostřednictvím vlastního nástroje měřit požadovanou dostupnost. O poskytnutí služby dodávky systému bude každý měsíc připraven ze strany Dodavatele „Akceptační protokol o poskytnutí služeb pro provizorní ISMS", který bude obsahovat minimálně následující informace:

- dostupnost služby dodávky za dané období;
- seznam výpadků s uvedením jejich doby a konkrétních časů;
- seznam provedených změn, apod.;
- seznam incidentů a problémů v gesci Dodavatele, které bezprostředně souvisely nebo se dotýkaly provozu provizorního ISMS.

2.4 Servisní odstávky systému

Servisní odstávky jsou přípustné pouze na základě schválení Zadavatele. Jednotlivá servisní odstávka nesmí přesáhnout 24 hodin.

Servisní odstávky musí být realizovány mimo nadefinovanou Provozní dobu systému. Servisní odstávky musí být přednostně plánovány na víkendy a svátky.

Typy servisních odstávek

- **plánované servisní odstávky** - plán servisních odstávek bude sestaven vždy na 12 měsíců dopředu (v případě posledního roku služby případně na kratší, zbývající období) a bude vždy předložen ke schválení Zadavatelem, a to nejpozději měsíc před zahájením poskytování služby, nebo na začátku 12. měsíce poskytování služby (tj. před zahájením dalšího roku poskytování služby).
- **mimořádné servisní odstávky** - mimořádné servisní odstávky, kromě odstávek pro řešení havarijních stavů, musí být plánovány minimálně jeden týden předem a oznámeny Zadavateli.

2.5 Incident management - servis a odstraňování vad

Vady budou kategorizovány minimálně následovně:

- **Vady kategorie A (vysoká, vyšší) -** stav, kdy závada v předmětu plnění Dodavatele způsobí více než jednomu uživateli nedostupné kritické funkce programového vybavení nebo jeho částí a tato nedostupnost znemožňuje zpracovat v požadované lhůtě výstup stanovený zákonem. Dále se jedná o stav, kdy výskyt vady má kritický dopad do funkčnosti systému, nebo hrozí poškození dat.
- **Vady kategorie B (střední) -** každý jiný stav, který neodpovídá podmínkám kategorie A nebo C.
- **Vady kategorie C (nízká, nižší) -** vybavení Dodavatele vykazuje drobnější vady nebo je podezření na vadu, ale základní funkčnost nebo jeho dílčí části je zachována.

- Dodavatel zahájí v termínu uvedeném v tabulce níže řešení vady, bezodkladně po přijetí požadavku Zadavatele. Dodavatel vyhodnotí ohlášený požadavek, zda se jedná nebo nejedná o vadu a podle toho dále postupuje.

Minimální požadavky na lhůty na odstranění vad:

Garance	Vada kategorie A	Vada kategorie B	Vada kategorie C
Zahájení řešení vady (doba od nahlášení do zahájení řešení vady).	Do 1 provozní hodiny služby od okamžiku nahlášení vady.	Do 2 provozních hodin služby od okamžiku nahlášení vady.	Do 4 provozních hodin služby od okamžiku nahlášení vady.
Zprovoznění vybavení alespoň náhradním způsobem pro zajištění jeho základních funkcí (tj. prozatímní, ne úplné odstranění vady).	Do 4 provozních hodin služby od okamžiku nahlášení vady.	N/A	N/A
Úplné odstranění vady.	Do 8 provozních hodin služby od okamžiku nahlášení vady, nejpozději však do 12:00 následujícího pracovního dne.	Do 36 provozních hodin služby od okamžiku nahlášení vady.	Do 48 provozních hodin služby od okamžiku nahlášení vady.

Pro účely výše uvedené tabulky je Provozní doba (a tedy provozní hodiny se počítají) pracovní dny, 8:00 až 17:00.

- V případě neodstranění vady v termínu uvedeném v tabulce výše je Dodavatel povinen na odstranění vady nepřetržitě pracovat až do úplného odstranění vady.
- Dodavatel po úplném odstranění vady/ukončení servisního zásahu vystaví protokol o zásahu. Protokol může být nahrazen zápisem vedeným elektronickou formou v nástroji pro Service Desk.
- Dodavatel vede evidenci všech poskytnutých služeb, hlášených vad a stavů jejich řešení a dále eviduje veškeré servisní zásahy v produkčním prostředí systému. Dodavatel předává výpis z takové evidence Dodavateli na měsíční bázi. Výpis představuje podklad pro fakturaci.

- Cena za poskytování Služeb zahrnuje též veškeré náklady Dodavatele, které smlouva předpokládá anebo které nejsou výslovně zmíněny, nicméně jejich potřeba musela být vzhledem k účelu Služeb Dodavateli známa.
- Služba bude akceptována na základě splnění Zadavatelem specifikovaných akceptačních kritérií.
- Dodavatel musí předem specifikovat požadovanou součinnost ze strany Zadavateli, která bude pro řešení hlášených závad vyžadována.
- Doba čekání na součinnost Zadavatele nebo třetí strany se nezapočítává do Doby reakce ani do Doby řešení vady. Reakční doby a doby řešení vad budou měřeny okamžikem prokazatelného nahlášení vady Zadavatelem Dodavateli prostřednictvím Service Desk.

2.6 Infrastruktura provizorního ISMS

Řešení infrastruktury musí dále zohledňovat požadavky v následující tabulce:

Požadavek	Popis požadavku
Bezpečnostní standardy	Architektura (návrh řešení) bude v souladu s požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti a souvisejících předpisů.
Ochrana osobních údajů	Architektura bude respektovat požadavky nařízení GDPR a souvisejících právních předpisů.
Kompatibilita	Architektura bude plně kompatibilní s veškerým SW a HW vybavením Zadavatele a ÚZSVM souvisejícím s touto veřejnou zakázkou, v technickém stavu stávajícího ISMS k 31. 12. 2019.
Standardizace	Architektura bude založena na rozšířených a celosvětově ověřených technologií.
Provoz významného informačního systému	Poskytování služeb dle předmětu plnění musí zohledňovat požadavky stanovené právními předpisy na provoz významného informačního systému dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, resp. prováděcí vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.