SPCSS
Státní pokladna
Centrum sdílených služeb

OBJEDNÁVKA č. 8

Ostatní činnosti
na základě Rámcové smlouvy
č. 105/2024-MSP-CES (SML2024144),
uzavřené dne 31.12.2024

Objednatel:
MINISTERSTVO SPRAVEDLNOSTI ČR
Vyšehradská 16, 128 10 Praha 2
Odbor informatiky

VÁŠ DOPIS č.j.:
ZE DNE:
NAŠE č. j.: MSP-116/2025-OI-OBJ/6

VYŘIZUJE: [redacted]
TEL.: [redacted]
FAX:
E-MAIL: [redacted]

Poskytovatel:
Státní pokladna
Centrum sdílených služeb, s.p.
Na Vápence 915/14
130 00 Praha 3
IČO: 03630919
DIČ: CZ03630919

Praha: 02.10.2025
Přílohy: 1

Objednávka Ostatních činností

Objednáváme tímto v souladu s Rámcovou smlouvou o poskytování Cloudové platformy AZURE a odborné podpory č.j. MSP-105/2024-MSP-CES („**Rámcová smlouva**“) Ostatní činnosti v tomto rozsahu:
Specifikace požadovaných Ostatních činností dle čl. 6.3.5 Rámcové smlouvy:
Příprava prostředí dle Přílohy č. 1 – HLD, která je součástí této Objednávky.

Termín zahájení a ukončení poskytování Ostatních činností:
Termín zahájení je stanoven účinností této Objednávky a termín ukončení do 5 pracovních dnů od účinnosti Objednávky.

Celková cena za Ostatní činnosti: 54 200 Kč bez DPH vč. rozpadu ceny:

1) **Plnění: Příprava prostředí dle Přílohy č. 1 - HLD**
   Jednotková cena: 54 200 Kč bez DPH (tj. 65 582 Kč s DPH)
   Počet jednotek: 1

Poznámka: Z důvodu potřeby sloučení Objednávky a Přílohy č. 1 HLD do jednoho dokumentu tak, aby byla zajištěna podmínka Poskytovatele připojit Přílohu jako nedílnou součást Objednávky.

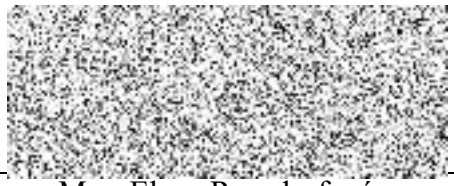
V návaznosti na výše uvedené rušíme Obj. č. 116/2025-OI-OBJ/3 a vyvářímе novou, totožnou Objednávku pod novým číslem jednacím MSP-116/2025-OI-OBJ/6 v souladu s požadavkem Poskytovatele.

Fakturace: na základě Akceptačního protokolu dle čl. 7.13 Rámcové smlouvy

Splatnost faktury 30 dnů. Při fakturaci uvádějte naše č. objednávky MSP- 116/2025-OI-OBJ/6 bez jeho uvedení bude faktura vrácena zpět. Fakturu zasílejte výhradně v elektronické podobě do datové schránky ministerstva č. kq4aawz, nebo na emailovou adresu: posta@msp.gov.cz.

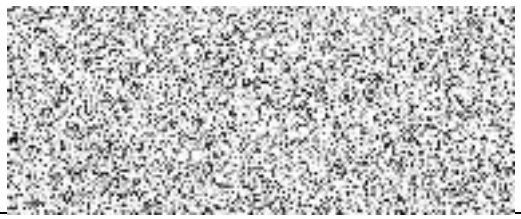
Objednávka bude v souladu s Rámcovou smlouvou uveřejněna v registru smluv.

S pozdravem



Mgr. Elena Ransdorfová
Ředitelka odboru informatiky
Ministerstvo spravedlnosti ČR

Za Poskytovatele:



Mgr. Jakub Richter
1. zástupce generálního ředitele
Státní pokladna Centrum sdílených služeb, s. p.

Příloha: Příloha č. 1 - HLD

Telefon
Fax:

Bankovní spojení: Česká národní banka
Praha 1, Na Příkopě 28
číslo účtu:

IČO:
00025429
5120001/0710
IBAN: CZ8807100000000005120001

Příloha č. 3

Státní pokladna Centrum sdílených služeb, s. p.
Na Vápence 915/14, Žižkov, 130 00 Praha 3

Počet listů: 20

Chatbot Justina

High level design

Obsah

Tento dokument High-level design představuje šablonu s kapitolami, které jsou nutným minimem pro popis dodávaného řešení ve fázi vyjednávání se zákazníkem. Dokument obsahuje stručný úvod, 2 diagramy cílového stavu dle požadavků zákazníka, a to:

- *diagram logického řešení*
- *diagram technologického řešení,*

Dále termíny realizace a participující týmy jak za SPCSS, tak za zákazníka, a to ve formě názvů oddělení dle organizačních řádů SPCSS a zákazníka.

1 Úvod

ISVR Chatbot Justina je nekritickou součástí systému ISVR.

Řešení představuje chatbot aplikaci, která umožňuje rychlé a efektivní zobrazení informací ve strukturované formě. Cílem je usnadnit uživatelům orientaci v rozsáhlých datech a zároveň zefektivnit komunikaci.

Vzhledem k tomu, že případný výpadek chatbotu nepředstavuje žádné riziko pro provoz ISVR a jedná se o doplňkovou službu, byl návrh provozního prostředí veden na maximální efektivitu, a to i za cenu omezení v oblasti monitoringu.

Předpokládá se, že po migraci systému ISVR do prostředí SPCSS Azura Cloud bude tento chatbot a jeho prostředky začleněn do systému bezpečnostních politik a prostředků ISVR. V současné době, vzhledem k rozsahu prostředí, požadovaného pro provoz chatbotu a s ohledem na nezávislost provozu ISVR na chatbotu by implementace bezpečnostních pravidel v plném rozsahu byla neekonomická.

1.1 Klasifikace aktiva

IS KIS – informační systém kritické informační infrastruktury	**VIS –** významný informační systém	**KS KII –** komunikační systém kritické informační infrastruktury	**IS ZS – informační** systém základní služby	**IS –** informační systém nebo síť elektronických komunikací
☐	☐	☐	☐	☒

Kapitola popíše klasifikaci aktiva dle ZoISVS a vyhlášky o CC a požadavků zadavatele.

ISVS	**BÚ 1**	**BÚ 2**	**BÚ 3**	**BÚ 4**
☒	☐	☐	☐	☐

1.2 Seznam použitých zkratek

Zkratka	**Vysvětlení**
ISVR	Informační systém veřejných rejstříků
ESM	Evidence skutečných majitelů
ESF	Evidence svěřenských fondů

1.3 Termíny realizace a zainteresované týmy

Kapitola popíše termíny realizace projektu v následující struktuře:

	Datum
Zahájení projektu:	Nebylo stanoveno v době tvorby HLD
Zahájení implementace:	Nebylo stanoveno v době tvorby HLD
Uvedení do provozu:	Nebylo stanoveno v době tvorby HLD
Ukončení projektu:	Nebylo stanoveno v době tvorby HLD
Ukončení provozu řešení:	Nebylo stanoveno v době tvorby HLD

1.3.1 Zainteresované týmy za stranu SPCSS:

1.3.1.1 SPOC SPCSS

Role	Jméno	e-mail	Telefon
IT Architekt			
Produktový manažer			

1.3.2 Zainteresované týmy za stranu zákazníka:

1.3.2.1 SPOC Zákazník

Role	Jméno	e-mail	Telefon
PM zákazníka			

1.3.2.2 SPOC Dodavatel

Role	Jméno	e-mail	Telefon
PM dodavatele			
Technik			

1.3.3 Provozní doba

Provozní doba	
8x5	☐
24x5	☐
24x7	☒

1.3.4 Celková roční dostupnost

Požadovaná dostupnost poskytovaného prostředí je určena požadavkem na celkovou dostupnost aplikace, která činí 97,62%.

	Typ SLA	Doba vyřešení kritické závady				ISVS
		4 hodiny	8 hodin	12 hodin	48 hodin	BÚ
☐	**96,16 %**	☐	☐	☐	☐	1
☒	**99,45 %**	☐	☒	☐	☐	2
☐	**99,9 %**	☐	☐	☐	☐	3
☐	**99,982 %**	☐	☐	☐	☐	3
☐	**99,99 %**	☐	☐	☐	☐	4

1.3.5 RPO/RTO

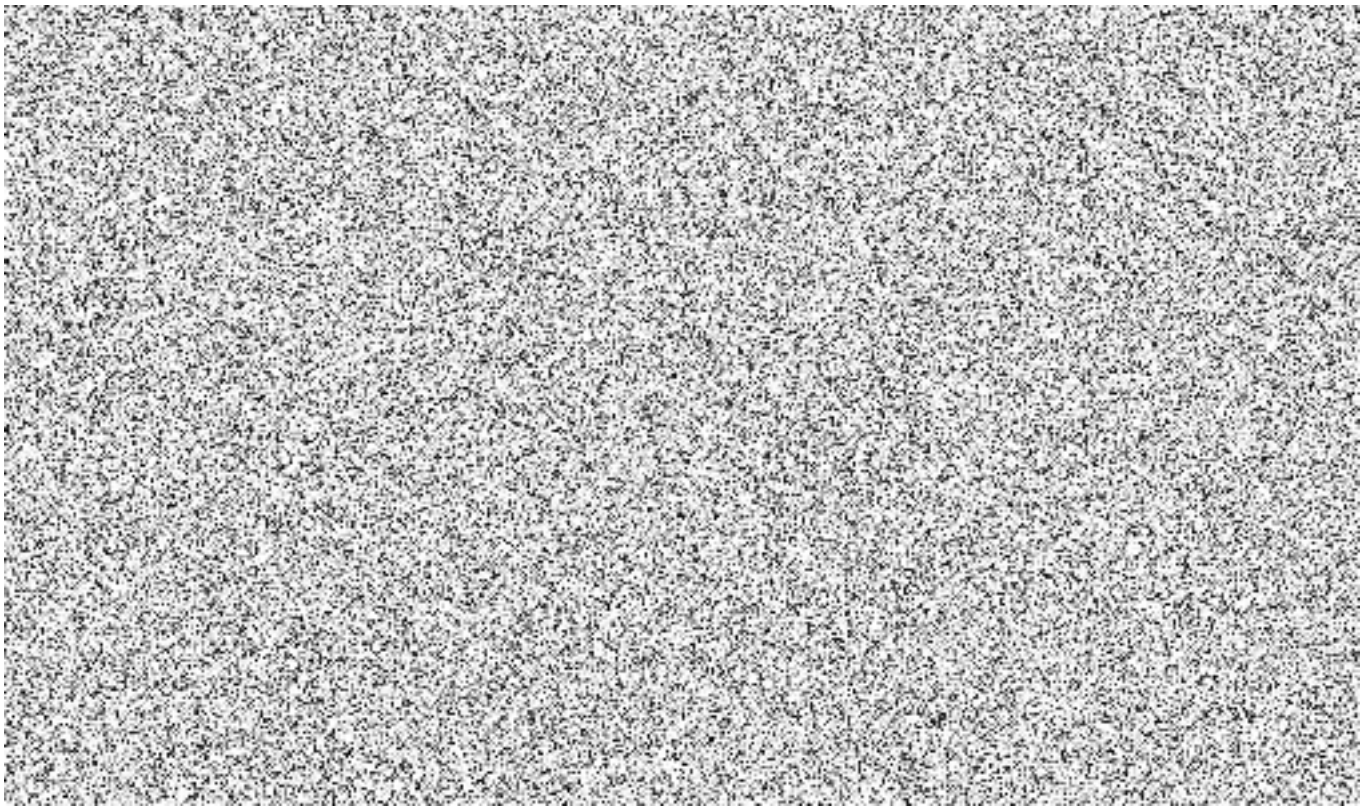
Typ SLA	Maximální možná délka	Popis
RPO	Není stanoveno	*cílový bod obnovení/zotavení*
RTO	Není stanoveno	*cílový čas/doba zotavení*

1.3.6 FQDN jméno pro aplikaci

Jméno aplikace	FQDN jméno
Privatni aplikace na spravu	chatbot-mgmt
CDN, skripty, styly, obrazky	chatbot-storage
Aplikace pro analytiku chatoba	chatbot-analytics
WS rozhrani chatbota	chatbot-webchatapi

2 Logický model řešení

2.1 Logický diagram



Popis aplikační architektury:

Chatbot se skládá z frontendové části, která je integrovaná do cílového webového portálu pomocí JavaScriptových skriptů, CSS stylů a doprovodných obrazových prvků. Frontend zajišťuje interaktivní uživatelské rozhraní a prostřednictvím WebSocket spojení komunikuje s backendem v reálném čase.

Backendové aplikace mají na starost samotnou logiku chatbota – obsluhují příchozí dotazy, vyhodnocují odpovědi, zajišťují reportování a správu obsahu. Součástí je také administrátorské rozhraní pro konfiguraci vzhledu a vlastností chatbota.

Veškerá aplikační data jsou ukládána v relačních databázích, které umožňují strukturované uchovávání informací a efektivní dotazování nad nimi.

Popis technologické architektury:

Jedná se o standardní cloudovou architekturu postavenou na virtuálním serveru s využitím pouze MS Azure cloudu.

3 Technické řešení

3.1 Technický diagram

Diagram a popis viz předcházející kapitola.

Projekt obsahuje 1 prostředí: PROD.

3.2 HW parametry

Bude využit pouze MS Azure Cloud.

3.2.1 Virtualizační platforma

Kapitola popíše platformu, na které bude služba poskytovaná. Pokud se jedná o ISVS, lze vybrat jen platformu, která je zapsaná v katalogu CC pro příslušnou Bezpečnostní úroveň.

MS Azure		MS AzureStack Hub		VM Ware	Power	Google cloud
BÚ 1-3		BÚ 4		BÚ 4	BÚ 4	BÚ 1-3
☒		☐		☐	☐	☐
VM ☒	K8s ☐	VM ☐	AKS ☐			

Virtualizační platforma je blíže specifikována v sekci „Compute" v kap. 3.2.1.1.

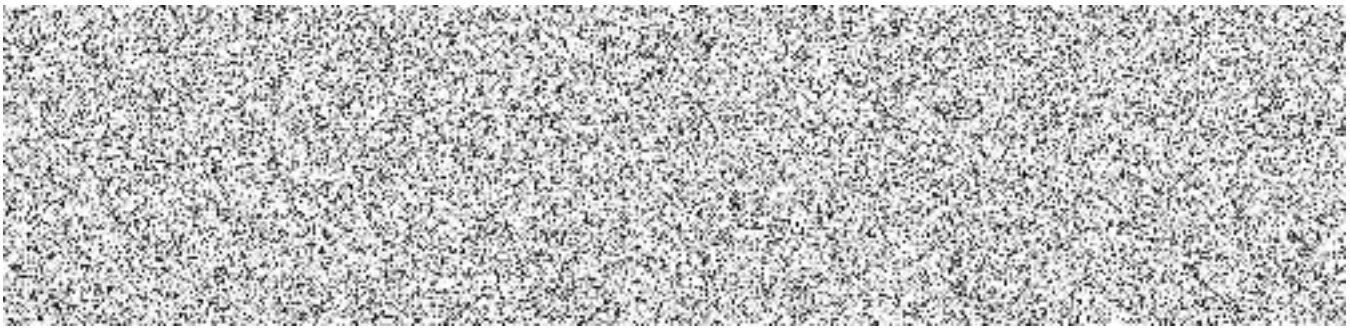
- 4 CPU
- 16GB RAM
- 128GiB HDD
- Linux (Ubuntu 22.04 nebo vyšší)

Dodavatel požaduje přístup do subscription, kde sám vytvoří prostředí pomocí IaC scriptů.

Poznámky:

Vzhledem k omezenému monitoringu pro tuto fázi implementace chatbotu odpovídá návrh BÚ 1.

3.2.1.1 MS Azure



Service category	Service type	Custom name	Region*	Description
Databases	Azure Database for PostgreSQL flexible server		Sweden Central	Flexibilní server Nasazení, Úroveň Burstable, 1 Standard_B2s (2 Virtuální jádra) x 730 Hodin (Průběžné platby), Úložiště – Premium SSD, úložiště 64 GiB, zřízené IOPS: 240, Zálohování – ZRS redundance, bez vysoké dostupnosti
Networking	Public IP address		Sweden Central	Staticka verejni IP adressa, SKU Standard
Networking	Virtual network		Sweden Central	Virtualni sit s pripojenym NIC Virtualniho serveru
Networking	Network Security Gateway		Sweden Central	NSG s nastavenymi Inbound rules pro rizeni pristupu na jednotlive porty serveru
Compute	Virtual Machine		Sweden Central	Linux Ubuntu 22.04 nebo vyssi, Standard B4ms nebo D4ads_v5 (4 vcpus, 16 GiB memory), Disk Standard SSD LRS 128 GB
Storage	Storage Account		Sweden Central	Replikace: LRS, Druh: StorageV2 (general purpose v2)

*V případě ISVS je nutné volit Region v závislosti na BÚ (pro BÚ 3 – Region EU, BÚ 1-2 bez omezení)

Navrhovaná konfigurace zdrojů:

Service category	Service type	Region	Description
Databáze	Azure Database for PostgreSQL	West Europe	Flexibilní server Nasazení, Úroveň Se zvládáním nárazových špiček, 1 B2S (2 Virtuální jádra) x 730 Hodin, Úložiště – Premium SSD, úložiště 64 GiB, 6 GiB Dodatečné úložiště zálohování – LRS redundance
Výpočetní prostředky	Virtual Machines	West Europe	1 D4ads v5 (4 vCPUs, 16 GB RAM) x 730 Hodin (Pay as you go), Linux, (Pay as you go); 1 managed disk – E10; Internet egress, 5 GB outbound data transfer from West Europe routed via Globální síť Microsoftu
Sítě	IP Addresses	West Europe	Standard (ARM), 6 statické IP adresy X 730 Hodin 16 předpon veřejných IP adres X 730 Hodin
Sítě	Virtual Network		West Europe (Virtuální síť 1): 0 GB – odchozí přenos dat; West Europe (Virtuální síť 2): 0 GB – odchozí přenos dat
Úložiště	Storage Accounts	West Europe	Block Blob Storage, Obecné účely V2, Plochý obor názvů LRS Redundance, Vrstva přístupu Hot, Kapacita 50 GB - Platte jenom za to, co využijete, 100 x 10 000 zápisů, 100 x 10 000 operací seznamu a vytvoření kontejneru, 100 x 10 000 operací čtení, 1 000 x 10 000 jiných operací. 1 000 GB načítání dat,1 000 GB zápis dat, Protokol FTP SSH zakázán

3.2.1.1.1 FinOps

Není specifikováno.

Služba	1 rok	3 roky	Prostředí + popis
Rezervace VM nebo VMSS	☐	☐	
Rezervace SQL	☐	☐	
Rezervace App service	☐	☐	
Rezervace Synapse Analytics	☐	☐	
Rezervace Data Factory	☐	☐	
Rezervace…	☐	☐	

Politiky a governance, které v rámci FinOps jdou nastavit. Ideální nastavení je pro TEST a DEV, ale může být použito i pro produkční prostředí.

Politika	Ano	Ne	Prostředí + popis
Vypínání všech VM po 19.hodině	☐	☐	
VM běží 24*5 (Po-Pá)	☐	☐	
VM běží 9*5 (Po-Pá: 8-17)	☐	☐	
VM SPOT Instance	☐	☐	
Azure Hybrid Benefit	☐	☐	
Azure EU nejlevnější region	☐	☐	

Budgety a rozpočty, které jdou nastavit na jednotlivá prostředí. A to jak se soft limitem, tak s hard limitem, kdy se po naplnění budgetu veškeré služby stopnou, než se obnoví limit další měsíc.

Prostředí	Budget	Hard limit	Soft Limit	Popis
Produkce	Zde si zákazník volí budget	☐	☐	

Automatické škálování znamená, že automaticky vytváříte nebo mažete zdroje dle utilizace a potřeby. Podmínky automatického škálování jsou dané dle pravidel, která si zvolí zákazník. Uplatňuje se u Virtual Machine Scale set (VMSS).

VMSS	Min	Max	Default	Scale out (nahoru)	Scale in (dolu)

Azure Storage Account Lifecycle Management se týká správy životního cyklu dat ukládaných v Azure Storage. Azure Storage poskytuje široké možnosti pro ukládání dat, včetně objektů, disků, souborů a front, a zahrnuje nástroje a politiky pro efektivní správu těchto dat a jejich optimalizaci.

Úroveň uložení dat	Minimální čas uložení dat bez dalších poplatku	Pravidlo Lifecycle
Hot	0 dní	--
Cool	30 dní	Po 30 dnech

Cold	90 dní	Po 60 dnech
Archive	180 dní	Po 150 dnech
Mazání dat		Kdy mazat data?

3.2.1.1.2 Poznámky

3.2.2 Storage

Kapitola popíše velikost a umístění použitých diskových systémů nad rámec základní konfigurace virtuálních serverů.

3.2.2.1 MS Azure

Typ Storage	Velikost	Umístění / Region*
Standard general		
Premium block blobs	Max. 50GB, pay per use	Dle umístění ostatních prvků
Premium file shares		
Premium page blobs		

*V případě ISVS je nutné volit Region v závislosti na BÚ (pro BÚ 3 – Region EU, BÚ 1-2 bez omezení)

3.2.3 Databáze

Kapitola popíše požadavky zákazníka a jeho řešení na využití databází.

3.2.3.1 Cloud (BÚ 3)

MS SQL	MS SQL cluster	Postgre SQL/Maria DB	Ostatní
☐	☐	☒	☐

3.2.3.2 Poznámky

Odhadovaná velikost databáze:

Flexibilní server Nasazení, Úroveň Burstable, 1 Standard_B2s (2 Virtuální jádra) x 730 Hodin (Průběžné platby), Úložiště – Premium SSD, úložiště 64 GiB, zřízené IOPS: 240, Zálohování – ZRS redundance, bez vysoké dostupnosti.

Viz sekce Databases v kap. 3.2.1.1.

3.2.4 FW troughput

Kapitola popíše zákazníkem celkový požadovaný troughput skrz FW SPCSS.

Síť	Rychlost připojení
INET	Mbps
ENET / Govbone	Mbps

3.2.5 VPN

Kapitola popíše privátní VPN tunel, případně site-2-sit tunely, které v rámci PoC vzniknou.

Typ VPN	Počet
Privat VPN	
S-2-S tunel	

3.2.6 HSM / KeyVault

Žádné požadavky. Pečetění je realizováno vzdálenou službou 602.

Typ zabezpečení certifikátem	ISVS*	
HSM	BÚ 1-4	☐
KeyVault	BÚ 1-3	☐

*V případě zajišťování provozu ISVS nebo jeho části, musí být aplikována funkcionalita šifrování.

3.2.7 Monitoring

3.2.7.1 On-premise

Provozní monitoring	Bezpečnostní monitoring*	Bezpečnostní monitoring databází*	Aplikační monitoring*
☐	☐	☐	☐

3.2.7.2 Cloud

Viz Poznámky níže.

Provozní monitoring	Bezpečnostní monitoring*	Bezpečnostní monitoring databází*	Aplikační monitoring*
☒	☒	☒	☐

3.2.7.3 Poznámky

Aplikační monitoring je realizován sondami Dodavatele.

Další monitoring (Provozní, Bezpečnostní, Bezpečnostní monitoring databází) nebude v této fázi projektu realizován s ohledem na nekritičnost chatbotu a na náklady, spojené s realizací monitoringu.

Kompletní monitoring bude implementován pro chatbot v rámci implementace ISVR v prostředí SPCSS Azure.

3.2.8 Logování

Kapitola popíše požadavky zákazníka na logování.

3.2.8.1 Cloud

Provozní logy	Bezpečnostní logy	Aplikační logy
☒	☒	☐

3.2.8.2 Poznámky

Provozní a bezpečnostní logy nebudou v této fázi implementace chatbotu poskytovány.

3.2.9 Zálohování

Nebylo specifikováno.

Typ prostředí	Typ zálohy	Četnost záloh	Retence záloh
PROD			

4 Bezpečnostní požadavky

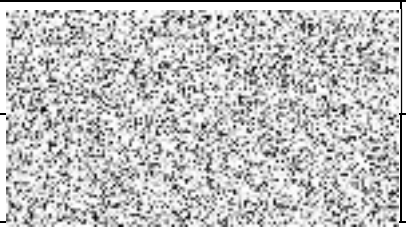
Jedná se o prvek KI, ale jeho veřejné části - z hlediska bezpečnosti se jedná primárně o dostupnost a pro některé části GDPR.

Požadovaná informace	Odpověď
Jedná se o službu pro IS, který podléhá ZoKB?	~~Ano~~ Ne
pokud Ano, o který druh se jedná?	☐ KII, ☐ VIS, ☐ Základní služba, ☐Digitální služba, ☐ Významná síť
Jedná se o podpůrnou službu pro IS, který podléhá ZoKB?	Ano ~~Ne~~

Požadovaná informace	Odpověď
Bude SPCSS smluvně jmenováno provozovatelem dle ZoKB?	~~Ano~~ Ne
Jaké povinnosti budou přeneseny na SPCSS a od koho?	• Některé povinnosti dle VoKB (které) • ~~Bezpečnostní monitoring~~ • ~~Provozní monitoring~~ • ~~Zálohování~~ • Disaster and recovery (pouze na IaaS) • Kontinuita provozu (pouze na IaaS) • ~~Incident response~~ • ~~Administrace a patchování~~ • ~~Řízení přístupu~~ • ~~Řízení dodavatelů~~
Jsou stanovena nezbytná opatření?	• Šifrování a síla klíčů • Rozsah logů dle §22 VoKB • Povolené protokoly • Požadavky na oddělení provozu • Míra dostupnosti (HA apod.) • IAM a pravidla přístupu, FSAD… • Loadbalancing • ~~DDOS ochrana~~ • ~~Požadavky na FW~~
Jaké budou parametry SLA?	• Response time PROD – 1h • Fix time A - 4h, B - 36 h, C - 216 h+ • Maximální výpadek 4hod/týden, dostupnost 97,6% (platí pro aplikační úroveň) • Incidenty • Doba uložení logů
Bude požadována ochrana před škodlivým kódem?	Ano ~~Ne~~
Bude požadována správa instalačních médií, zdrojového kódu apod.?	~~Ano~~ Ne
Bude požadována správa a dlouhodobé ukládání logů?	~~Ano~~ Ne
Jaký bude přístup ke službě?	• ~~VPN~~ • Aplikační FW • ~~Web v DMZ~~ • ~~CMS2~~ • Cloudová služba
Má zadavatel zaveden SŘBI (ISMS)?	Ano Ne
Zpřístupní Zadavatel relevantní dokumentaci?	Ano Ne
Zpřístupní Zadavatel PoA (prohlášení o aplikovatelnosti – výstup z analýzy rizik) atd?	Ano Ne

Požadovaná informace	Odpověď
Požaduje Zadavatel striktně využití jeho procesů a postupů?	~~Ano~~ Ne
Požaduje Zadavatel on-line přístup k logům?	Ano ~~Ne~~
Požaduje Zadavatel on-line přístup do SIEM?	Ano ~~Ne~~
Požaduje Zadavatel provedení penetračních testů?	Ano Ne

5 Podpisová doložka

Schvalovatel		
Role	**Jméno a příjmení**	**Datum a podpis**
Oddělení technické architektury a analytických činností:		
Odbor obchodu:		

Schvalovatel – zákazník		
Role	**Jméno a příjmení**	**Datum a podpis**

Informační proužek TLP pravidel

Příklad informačního proužku, který je vhodné umístit na konec dokumentu

Využití poskytnutých informací probíhá v souladu s metodikou **TLP** (Traffic Light Protocol) Více informací zde>>

Informační tabulka TLP pravidel

Příklad informační tabulky, kterou je vhodné umístit na konec dokumentu a vzhledem k její obsáhlosti i na novou stránku.

Podmínky využití poskytnutých informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách https://www.spcss.cz/tlp/). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Štítek	Podmínky použití
TLP: RED	**Informace není určena ke sdílení**, přístup je omezen na určené osoby (určuje původce/zdroj); **poskytnutí informace dalším subjektům uvnitř i vně organizace příjemcem lze učinit pouze s předchozím souhlasem původce/zdroje informace.**
TLP: AMBER+STRICT	**Sdílení informace je omezeno na určené osoby (příjemce) a jejich organizace** (určuje původce/zdroj) v souladu se zásadou **„potřebuje nezbytně znát"; příjemci nemohou dále sdílet tyto informace mimo svou organizaci bez předchozího souhlasu původce informace.**

TLP: AMBER	**Sdílení informace je omezeno na určené osoby (příjemce) a jejich organizace** (určuje původce/zdroj); **příjemci mohou sdílet tyto informace pouze s členy své organizace a s dodavateli nebo zákazníky**, kteří **nezbytně potřebují tyto informace znát**, aby se chránili nebo zabránili vzniku další škody; původce/zdroj informace může rozsah sdílení dále omezit.
TLP: GREEN	**Informace je určena k omezenému zveřejnění; omezeno na komunitu** (organizace příjemce a další partnerské subjekty příjemce informace), avšak **nikoliv s využitím veřejně dostupných komunikačních kanálů**; příjemce nesmí informaci šířit mimo určenou komunitu (určuje původce).
TLP: CLEAR	**Zveřejnění informace není omezeno**; tímto ustanovením není dotčeno omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran.

Komunita: skupina, která sdílí společné cíle, zkušenosti a neformální důvěryhodnost. Komunita může být různě rozsáhlá – může například zahrnovat všechny odborníky na kybernetickou bezpečnost v zemi (nebo v sektoru či regionu).

Organizace: skupina, která sdílí společnou příslušnost na základě formálního členství a je vázána společnými zásadami stanovenými organizací. Organizace může zahrnovat všechny členy organizace sdílející informace, ale jen zřídka je rozsáhlejší.

Zákazníci: osoby nebo subjekty, které využívají služby organizace.

Dodavatelé: osoby nebo subjekty, které organizaci dodávají služby či zboží.