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

Počet listů: 29

MZV Landing zóna TEST

High level design

Datum 29.8.2025

Obsah

1 Úvod ... 3
1.1 Klasifikace aktiva ... 3
1.2 Úroveň poskytovaných služeb ... 3
1.3 Seznam použitých zkratek ... 3
1.4 Termíny realizace a zainteresované týmy ... 4
1.4.1 Zainteresované týmy za stranu SPCSS: ... 4
1.4.2 Zainteresované týmy za stranu zákazníka: ... 5
1.4.3 Provozní doba ... 5
1.4.4 Celková roční dostupnost ... 6
1.4.5 [redacted] ... 6
1.4.6 FQDN jméno pro aplikaci ... 6
2 Logický model řešení ... 7
2.1 Logický diagram ... 7
3 Technické řešení ... 8
3.1 Technický diagram ... 11
3.2 HW parametry ... 13
3.2.1 Virtualizační platforma ... 13
3.2.2 Storage ... 20
3.2.3 Databáze ... 21
3.2.4 Síťová platforma ... 22
3.2.5 HSM / KeyVault ... 22
3.2.6 Monitoring ... 23
3.2.7 Logování ... 24
3.2.8 Zálohování ... 25
4 Bezpečnostní požadavky ... 25
5 Podpisová doložka ... 28
Informační proužek TLP pravidel ... 29
Informační tabulka TLP pravidel ... 29

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

Kapitola popíše hlavní náplň služby/řešení a jakým způsobem je služba/řešení poskytováno zákazníkovi a jaká jsou požadovaná SLA.

1.1 Klasifikace aktiva

Kapitola popíše klasifikaci aktiva dle VoKB a požadavků zadavatele

Landing zona zajišťuje konektivitu připojení pro služby MZV, které jsou v režimu BÚ 4.

Technologie Cisco a Fortinet.

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 Úroveň poskytovaných služeb

Kapitola popíše úroveň požadavků zadavatele na poskytování služeb

IaaS	**PaaS**
☒	☐

1.3 Seznam použitých zkratek

Uveďte seznam všech použitých zkratek v dokumentu. Jejich vysvětlení musí být pochopitelné pro všechny role zúčastněné na jednáních se zákazníkem.

Zkratka	**Vysvětlení**
[redacted]	

1.4 Termíny realizace a zainteresované týmy

Kapitola popíše termíny realizace projektu v následující struktuře:

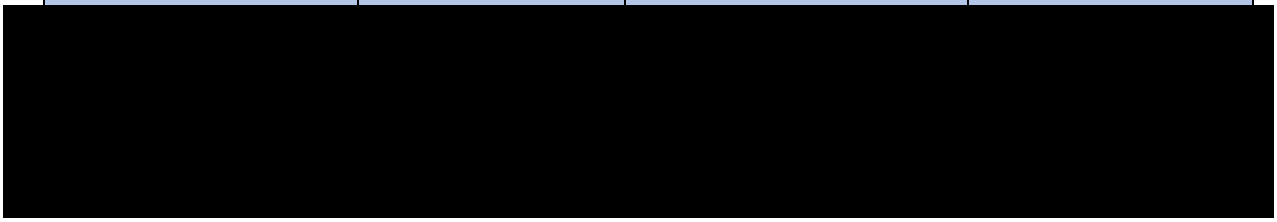
	Datum
Zahájení projektu :	2Q 2025
Zahájení implementace:	2Q 2025
Uvedení do provozu:	Do 31. 10. 2025
Ukončení projektu:	N/A
Ukončení provozu řešení:	Nerelevantní

1.4.1 Zainteresované týmy za stranu SPCSS:

[tým SPCSS, který zakázku připravuje zde vloží zainteresované role a oddělení za stranu SPCSS]

1.4.1.1 SPOC SPCSS

Role	**Jméno**	**e-mail**	**Telefon**



1.4.2 Zainteresované týmy za stranu zákazníka:

[tým zákazníka, který zakázku připravuje zde vloží zainteresované role a oddělení za stranu zákazníka]

1.4.2.1 SPOC Zákazník

Role	Jméno	e-mail	Telefon
[redacted]			

1.4.2.2 SPOC Dodavatel

Role	Jméno	e-mail	Telefon

1.4.3 Provozní doba

Kapitola popíše požadovanou provozní dobu zákazníkem

Provozní doba	
8x5	☒
24x5	☐
24x7	☐

1.4.4 Celková roční dostupnost

[redacted]

	Typ SLA		Doba vyřešení kritické závady - TEST				ISVS
		4 hodiny	8 hodin	12 hodin	24 hodin	48 hodin	BÚ
☒	**96,16 %**	☐	☐	☐	☒	☐	1
☐	**99,45 %**	☐	☐	☐	☐	☐	2
☐	**99,9 %**	☐	☐	☐	☐	☐	3
☐	**99,982 %**	☐	☐	☐	☐	☐	3
☐	**99,99 %**	☐	☐	☐	☐	☐	4

[redacted]

1.4.6 FQDN jméno pro aplikaci

Kapitola popíše zákazníkem požadované FQDN jméno pro provozovanou aplikaci

.

Jméno aplikace	FQDN jméno
-	-

2 Logický model řešení

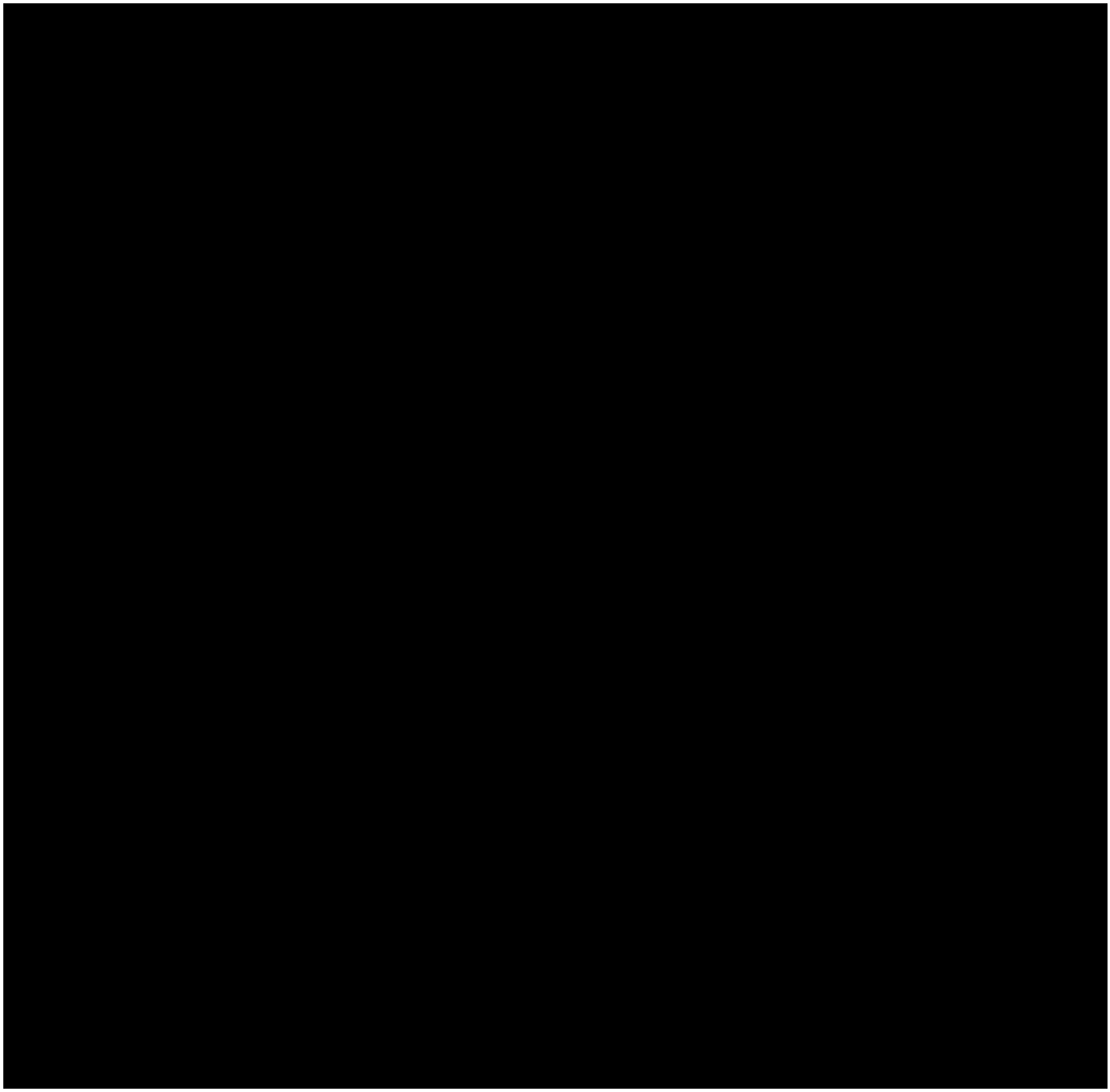
2.1 Logický diagram

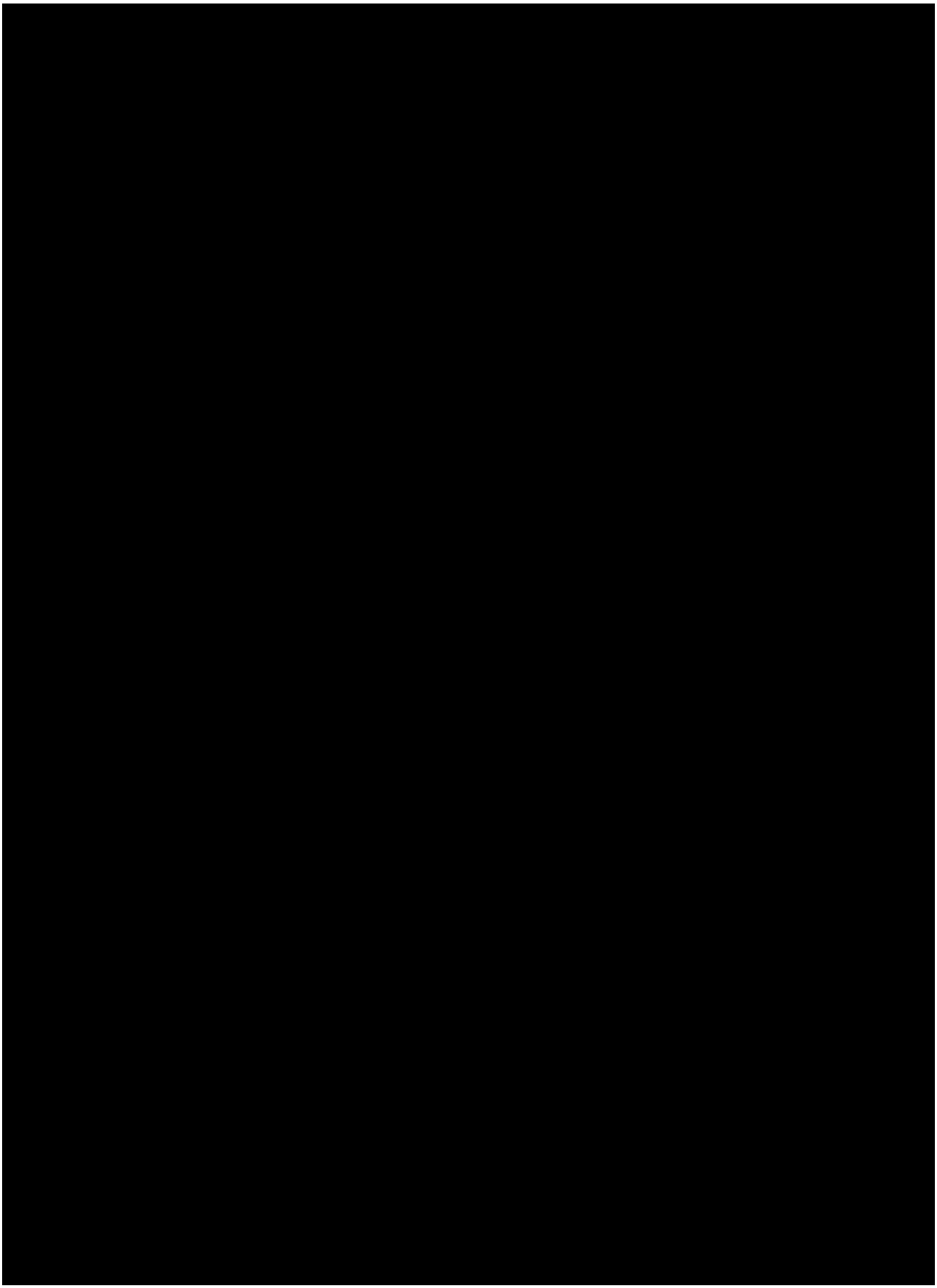
Kapitola bude obsahovat diagram logického modelu dle metodiky TOGAF s moduly řešení včetně architektonických vrstev v produkčním prostředí. Každý diagram musí mít popisek, co znázorňuje. Diagramů může být více, pokud to rozsah popisu nabídky vyžaduje.

Diagram musí jednoznačně určit prvky na jednotlivých vrstvách (business, aplikační a technologická) a jejich vazby:

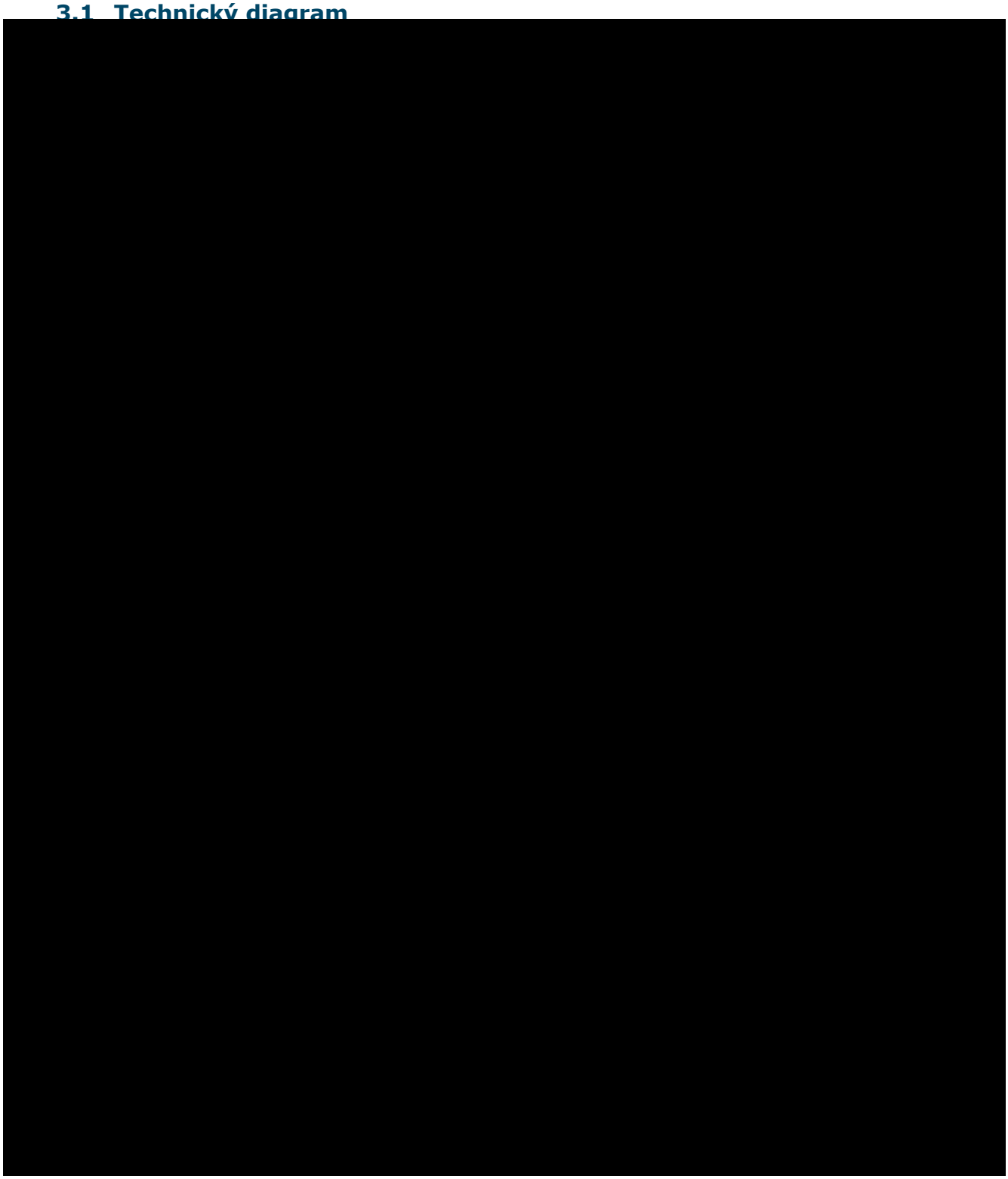
- *Organizace, které k řešení přistupují (organizace, která řešení požaduje (např. z důvodu agendy), SPCSS jako poskytovatel housingu/hostingu, dodavatel, pokud je v řešení zainteresován)*
- *Role v organizacích, které k řešení přistupují*
- *Způsob přístupu k infrastruktuře (Govbone, internet)*
- *Aplikaci/aplikace a její/jejich funkce*
- *infrastrukturu*

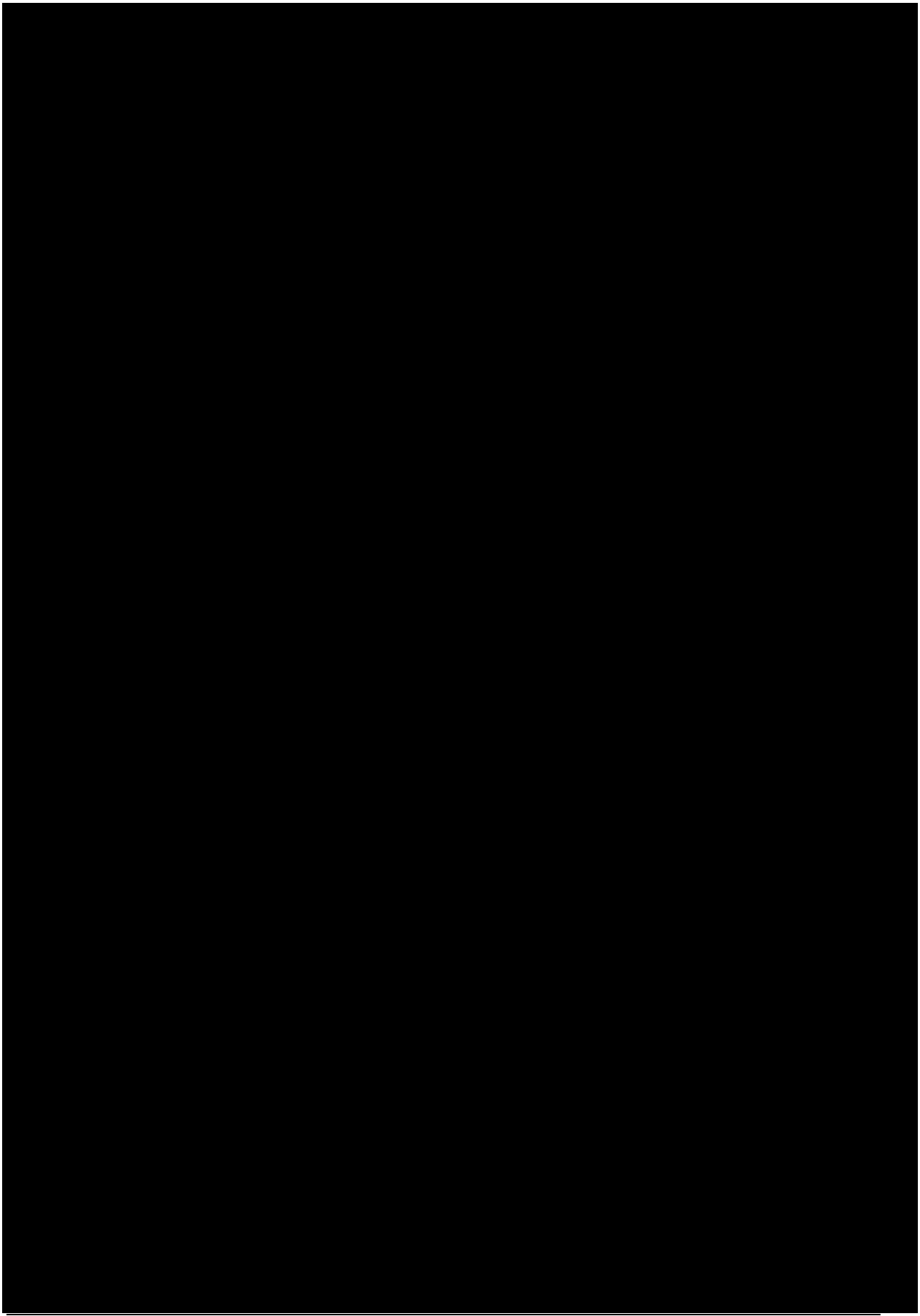
3 Technické řešení





3.1 Technický diagram



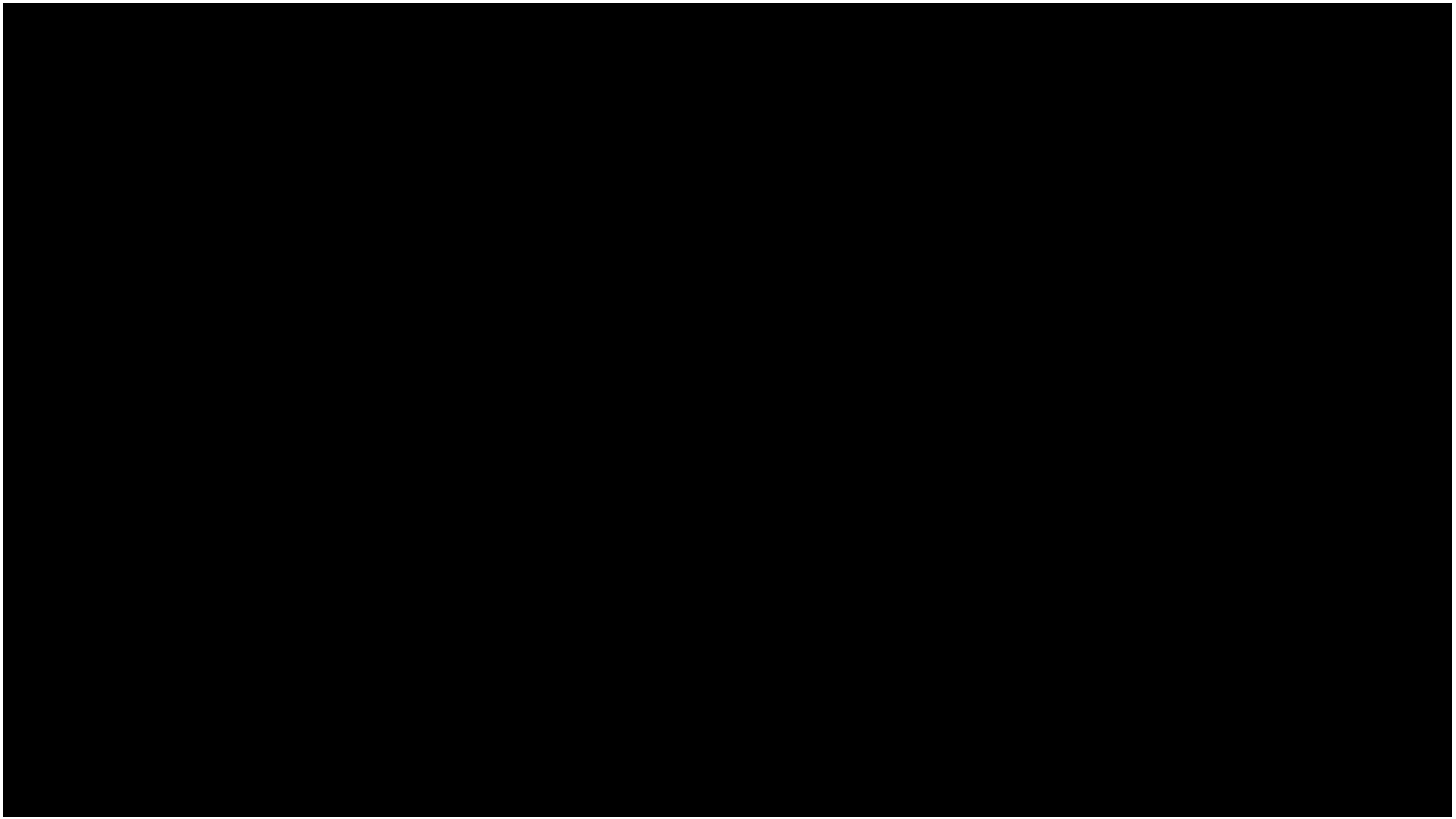


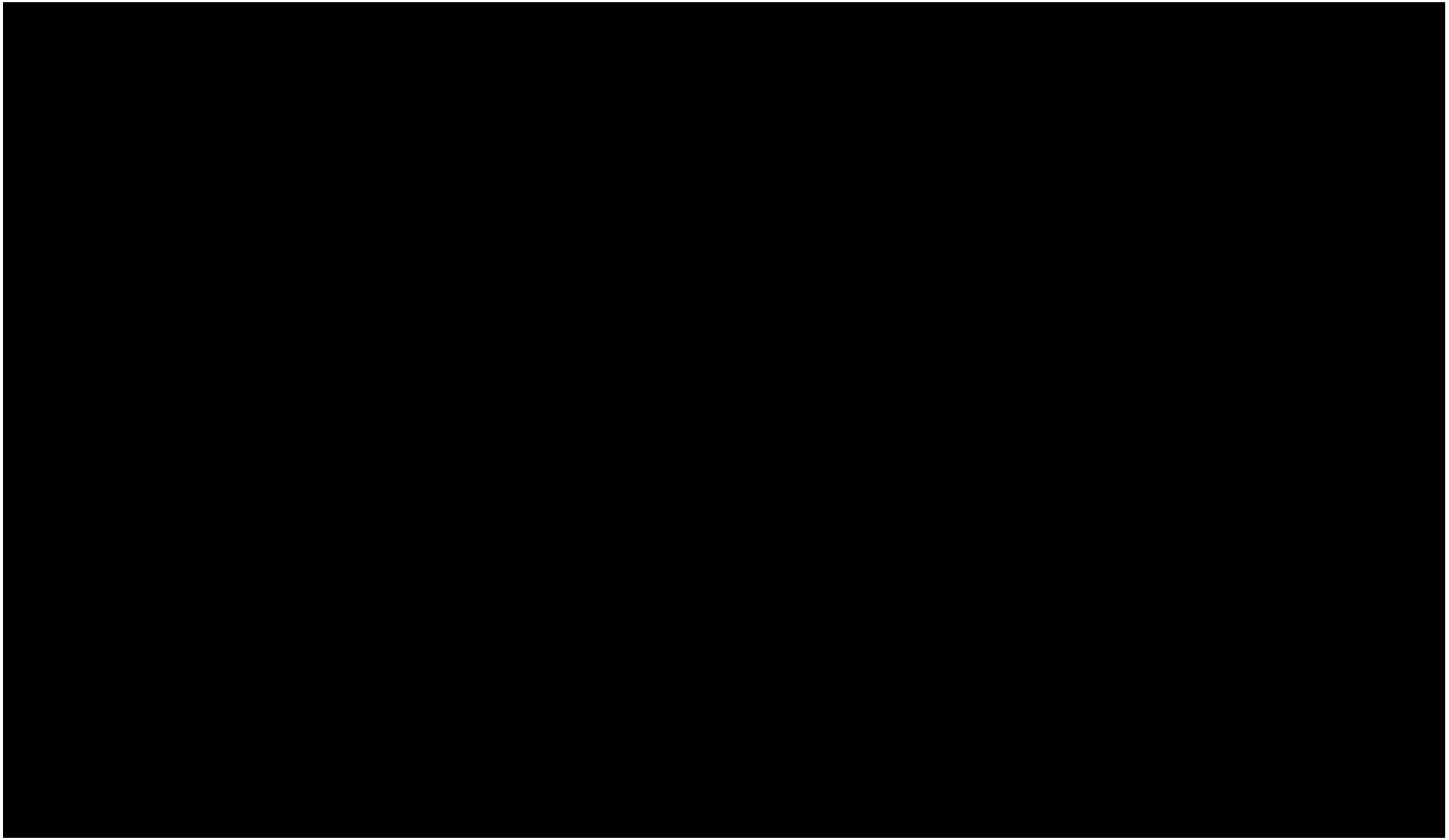
3.2 HW parametry

Kapitola popíše HW parametry jednotlivých prostředí v jednotlivých datových centrech.

3.2.1 Virtualizační platforma

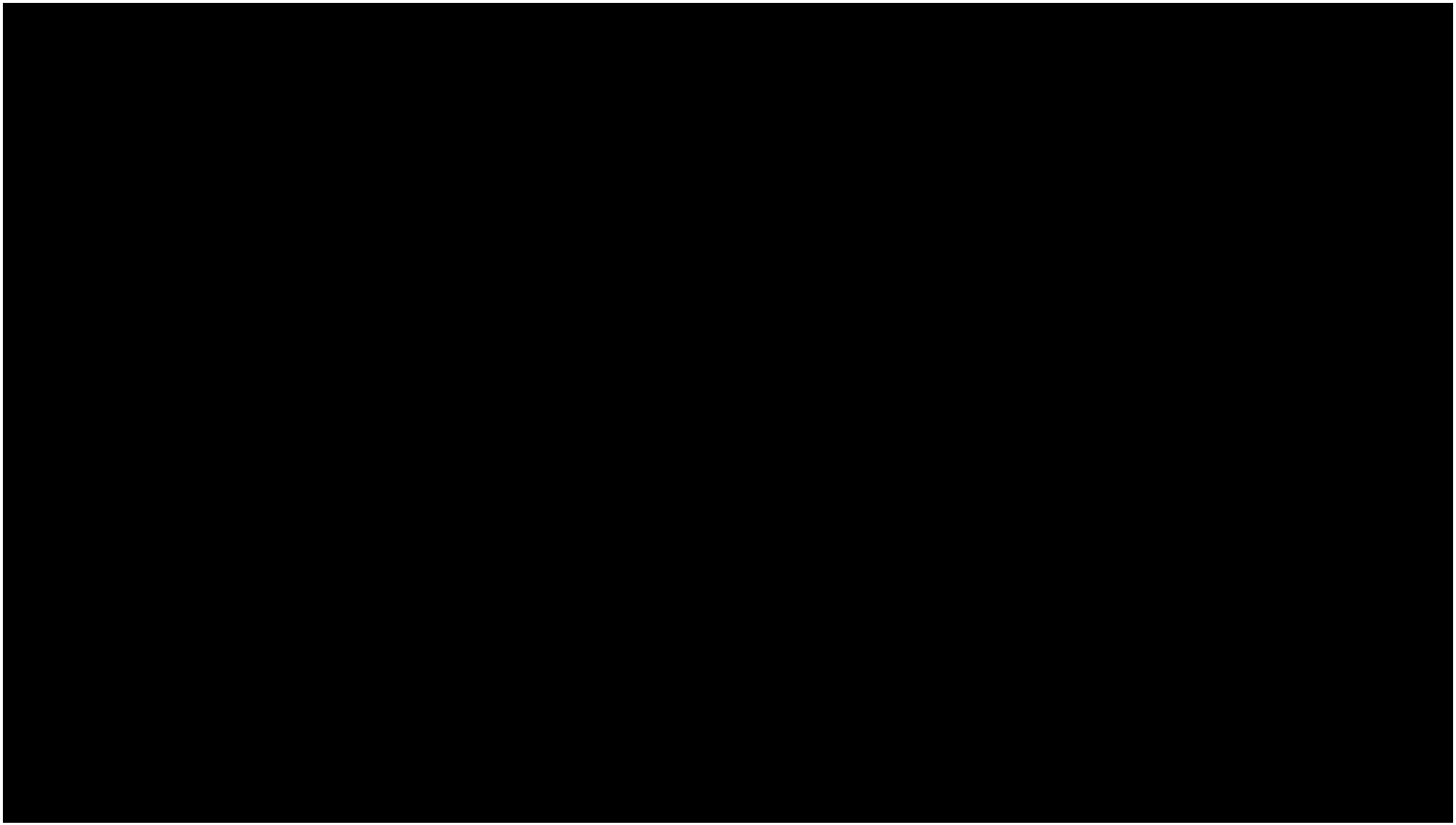
Kapitola popíše platformu na které bude služba poskytovaná. Pokud se jedná o ISVS, lze vybrat jen platformu, která je zapsaná v katalogu CC pro příslušnou Bezpečnostní úroveň.





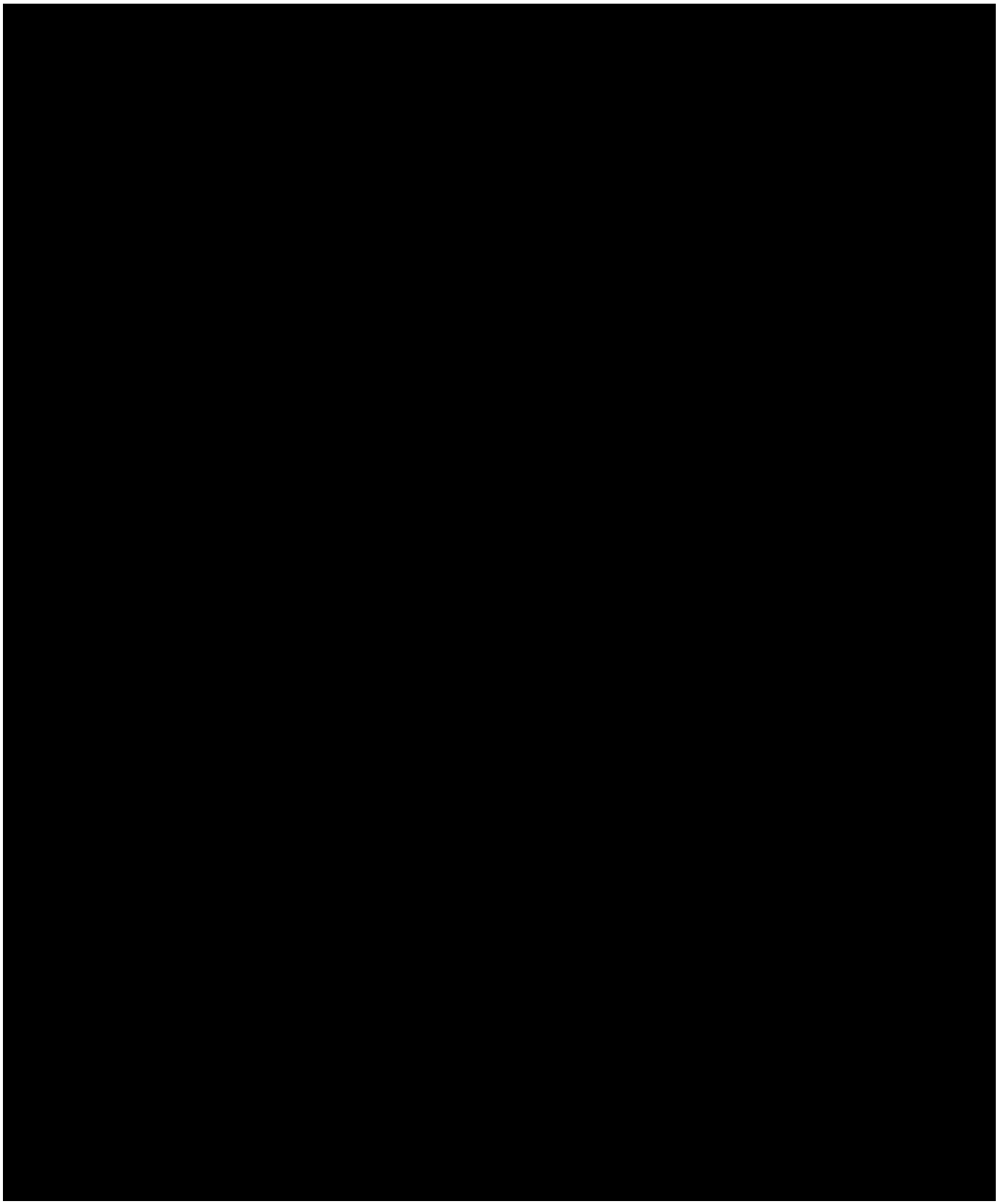
3.2.1.1.2 Poznámky

Není relevantní.



3.2.2 Storage

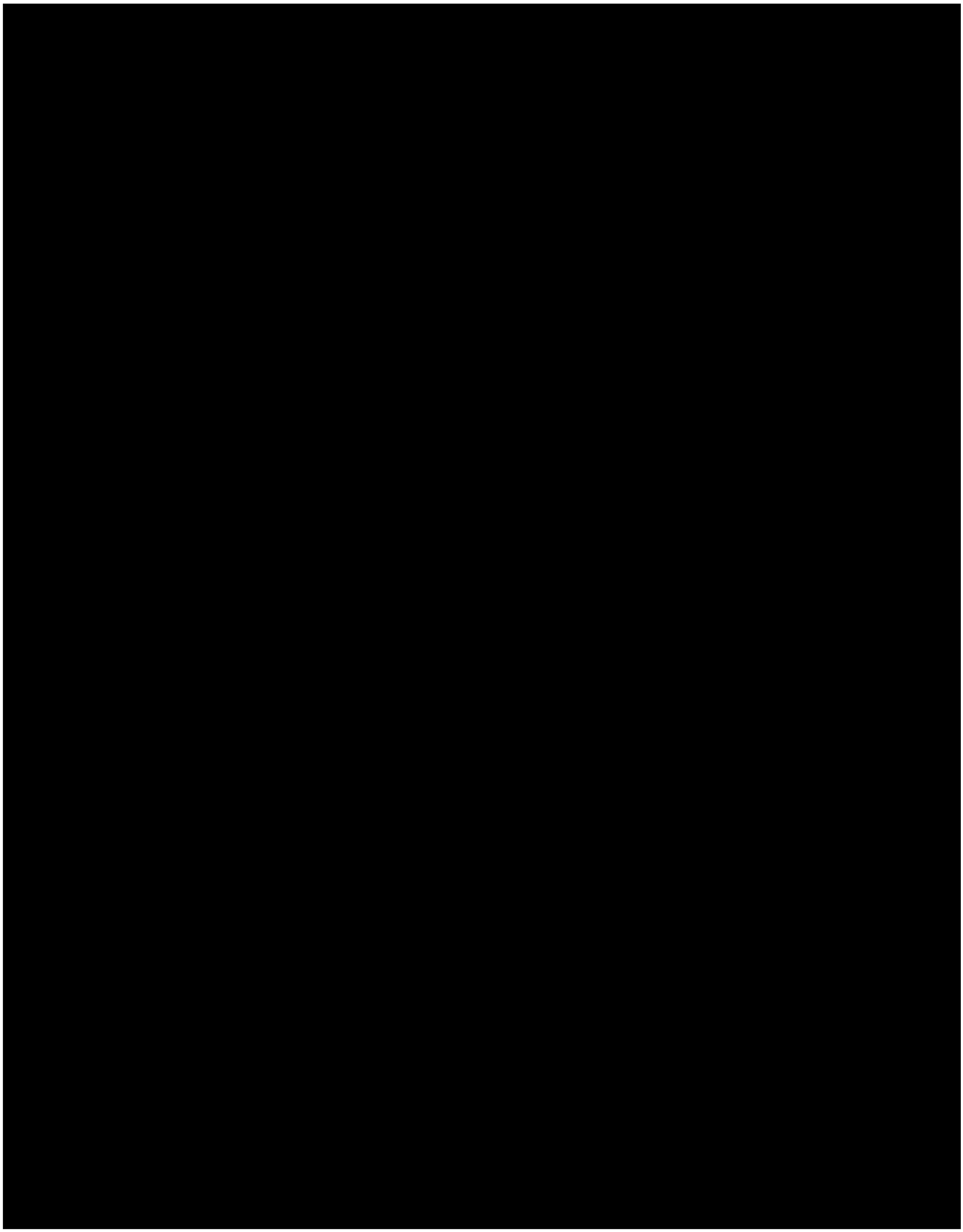
Kapitola popíše velikost a umístění použitých diskových systémů nad rámec základní konfigurace virtuálních serverů, či Kubernetes clusterů.



3.2.3.3 Poznámky

Kapitola popíše případné podrobnosti a požadavky na řešení DB.

3.2.4 Síťová platforma



3.2.6 Monitoring

*Kapitola popíše požadavky systému na jednotlivé typy monitoringu, které zákazník požaduje. *V případě provozu ISVS nebo jeho části, musí být implementován Provozní monitoring, Bezpečnostní monitoring a Bezpečnostní monitoring databází pro BÚ (2-4). Platí pro On-premis i Cloud.*

3.2.6.2 Cloud

[redacted]

3.2.6.3 Poznámky

Kapitola popíše případné podrobnosti a požadavky na řešení jednotlivých typů monitoringu.

[redacted]

3.2.7 Logování

Kapitola popíše požadavky zákazníka na logování.

[redacted]

3.2.7.2 Cloud

[redacted]

3.2.7.3 Poznámky

Kapitola popíše případné podrobnosti a požadavky na zasílání logů do SIEM/Qradaru.

[redacted]

[redacted]

3.2.8 Zálohování

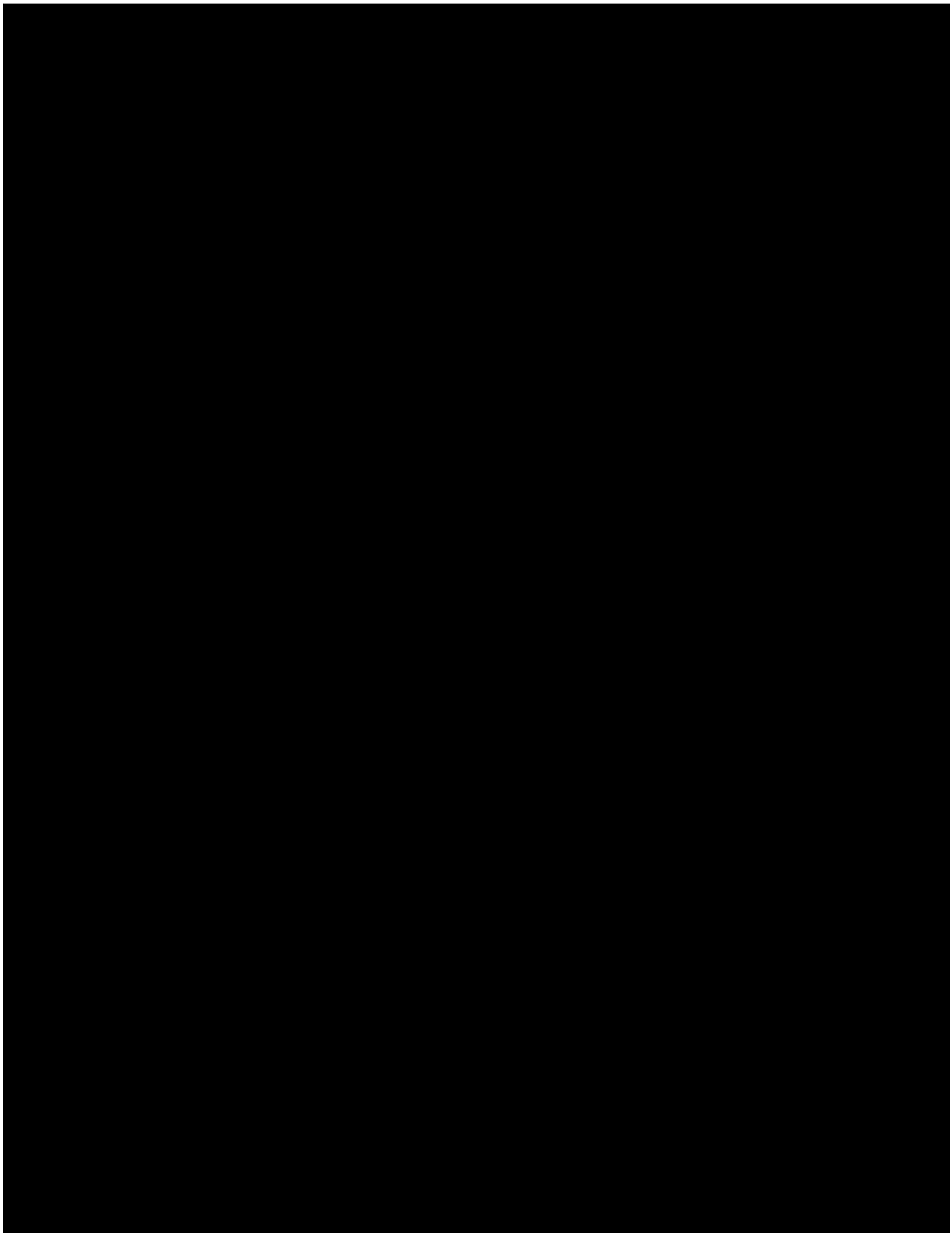
Kapitola popíše způsob, četnost a retenci záloh požadovaných systémem/dodavatelem aplikace
Typ zálohy – snapshot, nebo souborová záloha
Četnost záloh – jak často bude záloha vykonávaná
Retence záloh – jak dlouhou bude záloha uchovaná, než se smaže. Údaj je ve dnech

[redacted]

4 Bezpečnostní požadavky

Kapitola popíše požadavky zákazníka na bezpečnost, bezpečnostní a provozní monitoring.
Primárně sbírané informace jsou připraveny formou následující tabulky, kde nehodící se škrtněte.

[redacted]



5 Podpisová doložka

Zhotovitel		
Role	**Jméno a příjmení**	**Datum a podpis**
IT architekt:		

Předschvalovatel		
Role	**Jméno a příjmení**	**Datum a podpis**
Vedoucí oddělení správy MS:		
Vedoucí oddělení správy UNIX/Linux:		
Vedoucí správy síťových komunikací:		
Vedoucí oddělení databází:		
Vedoucí aplikační podpory:		
Vedoucí oddělení zálohování a storage		
Architekt KB:		

Schvalovatel		
Role	**Jméno a příjmení**	**Datum a podpis**
Vedoucí oddělení technické architektury a analytických činností:		

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.