



MZV Landing zóna PROD

High level design

Verze	Upraveno dne	Poznámka
1.0	02.09.2025	

Obsah

1	Úvod	3
1.1	Klasifikace aktiva	3
1.2	Úroveň poskytovaných služeb.....	3
1.3	Seznam použitých zkratk	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:	4
1.4.3	Provozní doba.....	5
1.4.4	Celková roční dostupnost	5
1.4.6	FQDN jméno pro aplikaci.....	6
2	Logický model řešení	7
2.1	Logický diagram	7
3	Technické řešení.....	7
3.1	Technický diagram.....	9
3.2	HW parametry.....	11
3.2.1	Virtualizační platforma	11
3.2.2	Storage	17
3.2.3	Databáze	18
3.2.4	Síťová platforma	18
3.2.5	HSM / KeyVault	19
3.2.6	Monitoring	19
3.2.7	Logování.....	20
3.2.8	Zálohování.....	21
4	Bezpečnostní požadavky.....	21
5	Podpisová doložka	24
	Informační proužek TLP pravidel.....	25
	Informační tabulka TLP pravidel	25

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

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
☐	☐	☐	☐	☒

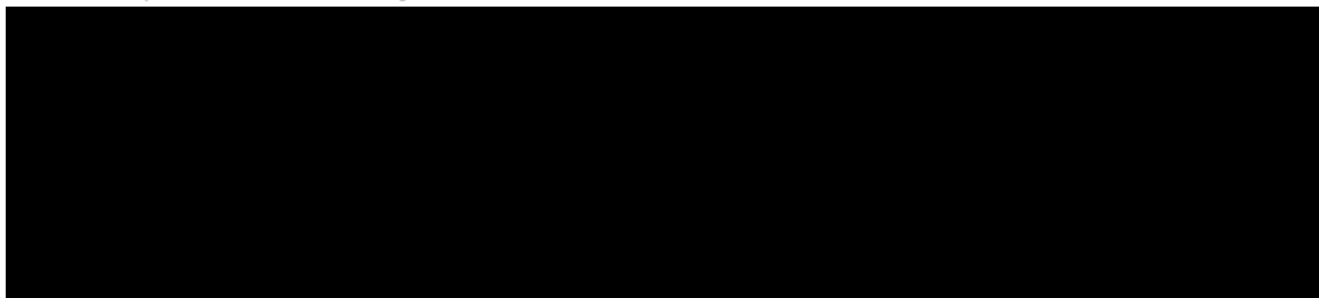
1.2 Úroveň poskytovaných služeb

Kapitola popíše úroveň požadavků zadavatele na poskytování služeb

IaaS	PaaS
☒	☐

1.3 Seznam použitých zkratk

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



1.4 Termíny realizace a zainteresované týmy

Kapitola popisuje termíny realizace projektu v následující struktuře:

	Datum
Zahájení projektu :	2Q 2025
Zahájení implementace:	2Q 2025
Uvedení do provozu:	3Q 2025
Ukončení projektu:	4Q 2025
Ukončení provozu řešení:	Nerelevantní

1.4.1 Zainteresované týmy za stranu SPCSS:

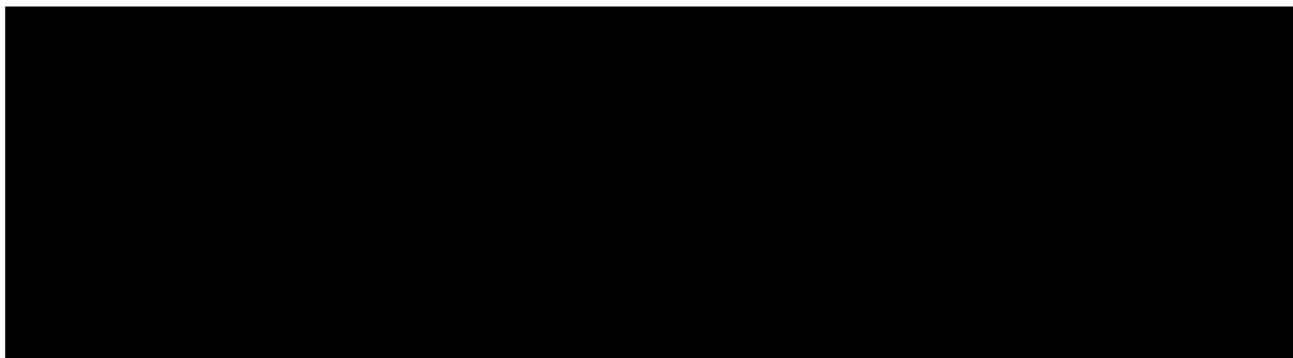
[tým SPCSS, který zakázku připravuje zde vloží zainteresované role a oddělení za stranu SPCSS]

1.4.1.1 SPOC SPCSS

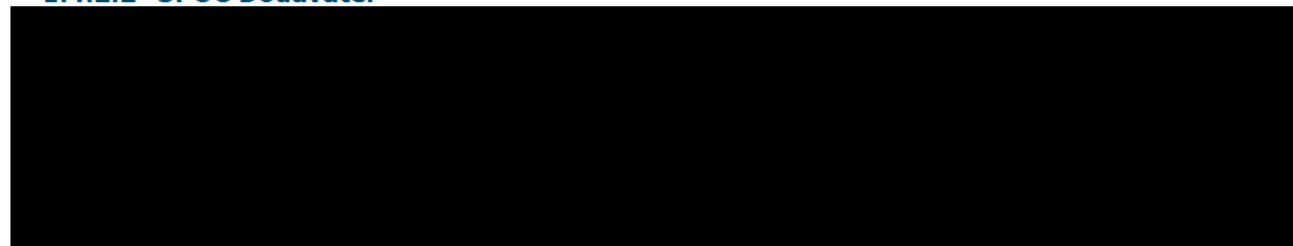
1.4.2 Zainteresované týmy za stranu zákazníka:

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

1.4.2.1 SPOC Zákazník



1.4.2.2 SPOC Dodavatel



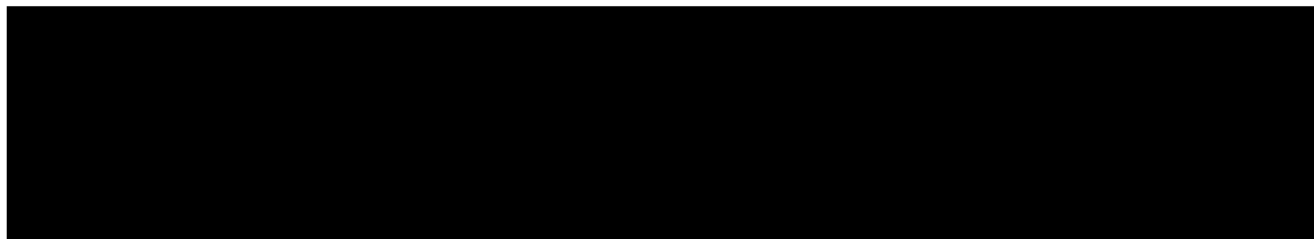
1.4.3 Provozní doba

Kapitola popíše požadovanou provozní dobu zákazníkem

Provozní doba	
8x5	☐
24x5	☐
24x7	☒

1.4.4 Celková roční dostupnost

Kapitola popíše zákazníkem požadovanou celkovou roční dostupnost, a to pro každé požadované prostředí zvlášť. Pro jiná, než produkční prostředí není třeba zohledňovat bezpečnostní úroveň IS.



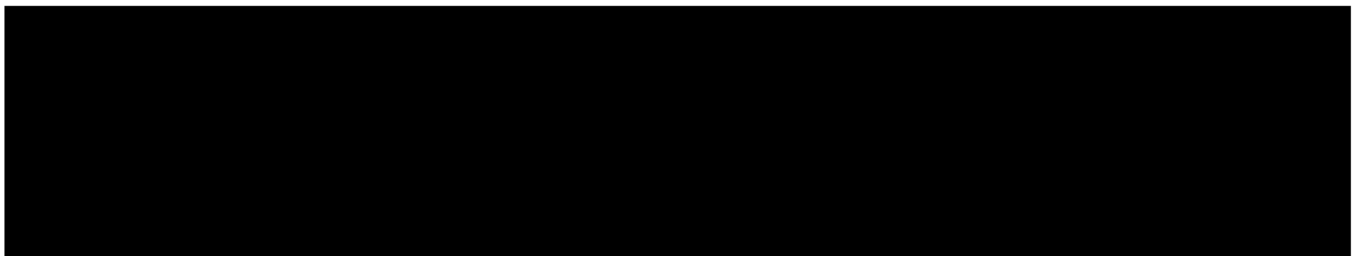
PROD prostředí

Typ SLA	Doba vyřešení kritické závady - PROD				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

1.4.5 RPO/RTO

Kapitola popíše zákazníkem požadované doby na dobu a cílový obnovení.



1.4.6 FQDN jméno pro aplikaci

Kapitola popíše zákazníkem požadované FQDN jméno pro provozovanou aplikaci

Jméno aplikace	FQDN jméno
-	-

2 Logický model řešení

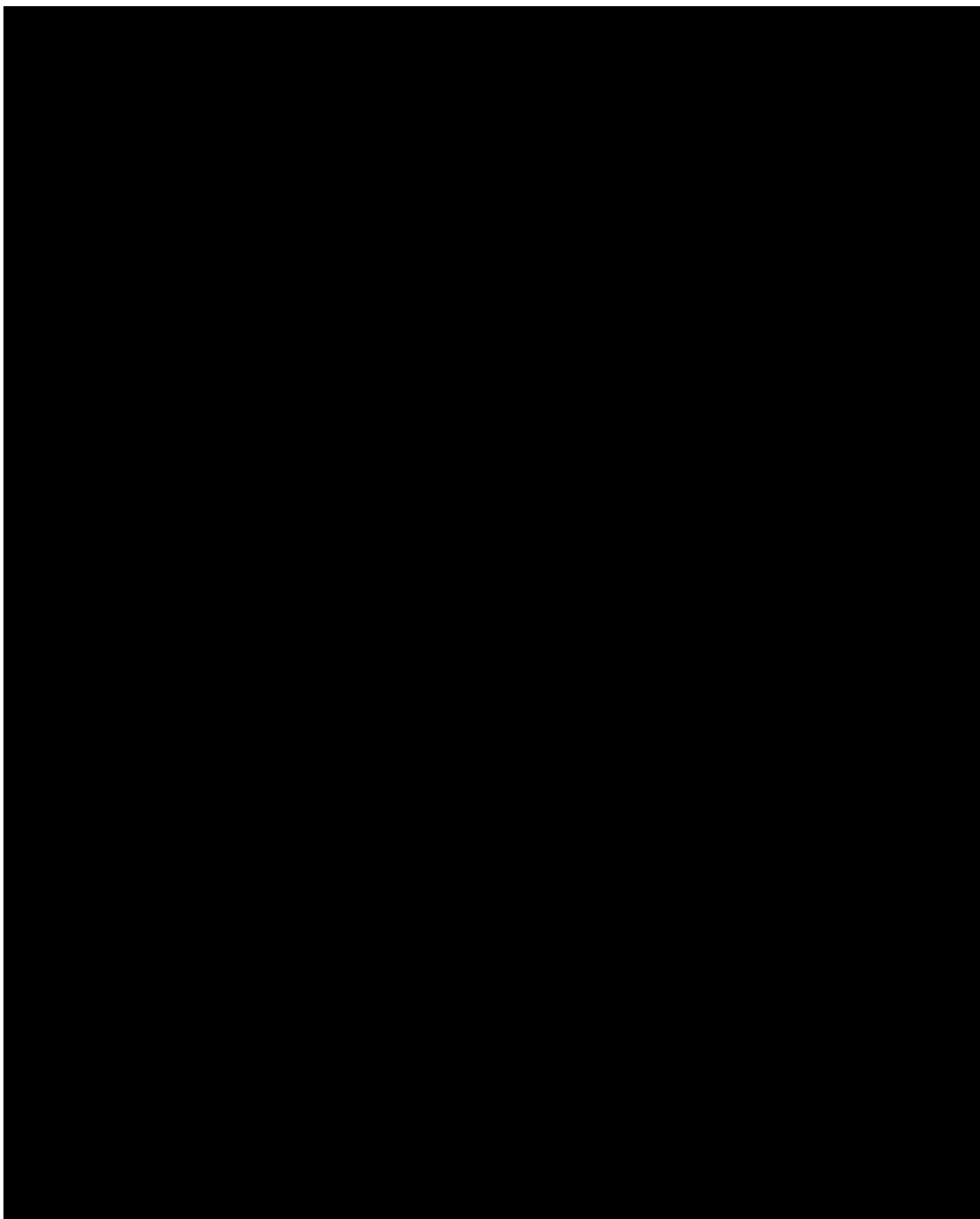
2.1 Logický diagram

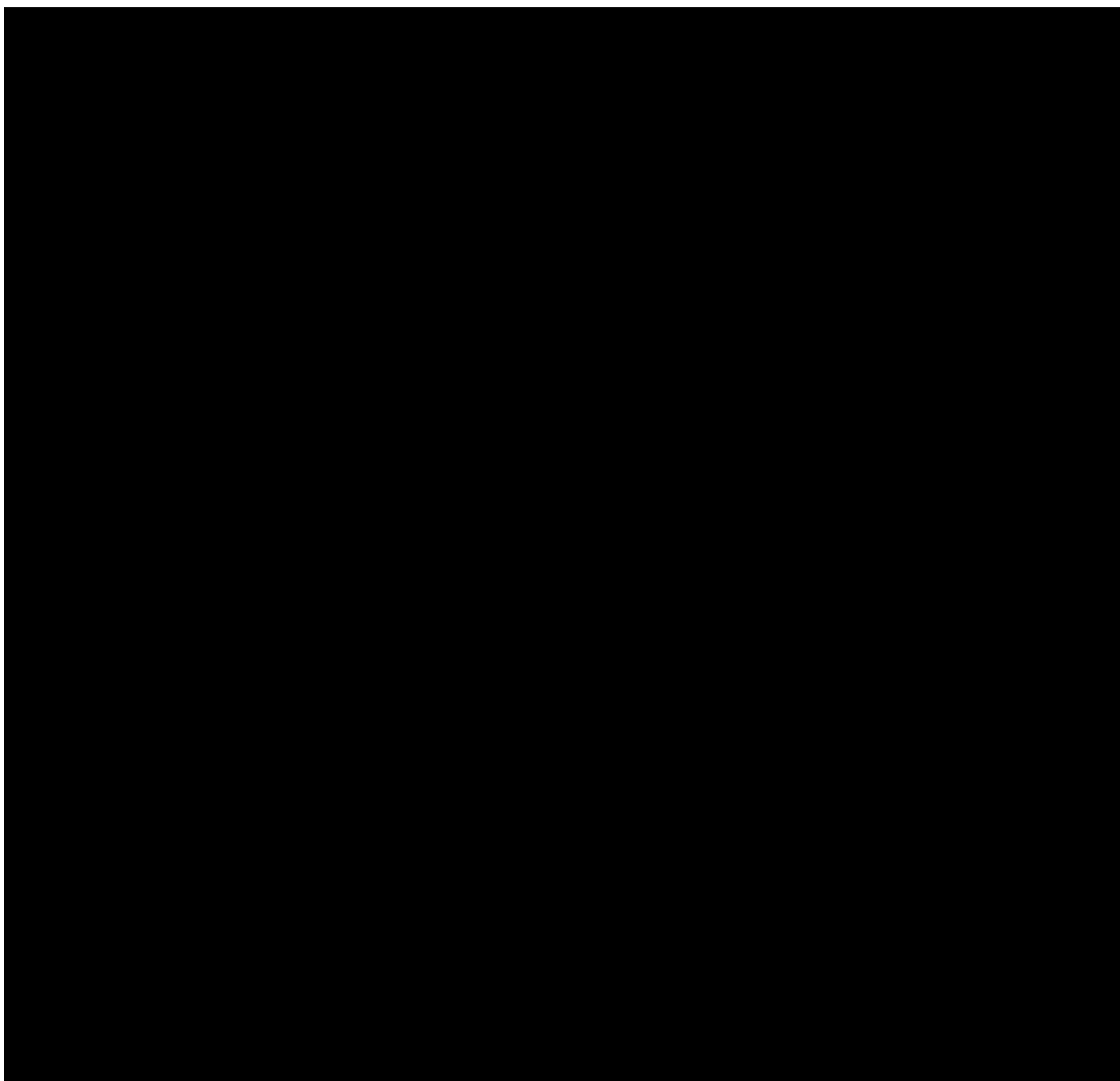
Kapitola bude obsahovat diagram logického modelu dle metodiky TOGAF s moduly řešení včetně architektonických vrstev v produkčním prostředí. Každý diagram musí mít popis, co znázorňuje. Diagramů může být více, pokud to rozsah popisu nabídky vyžaduje.

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

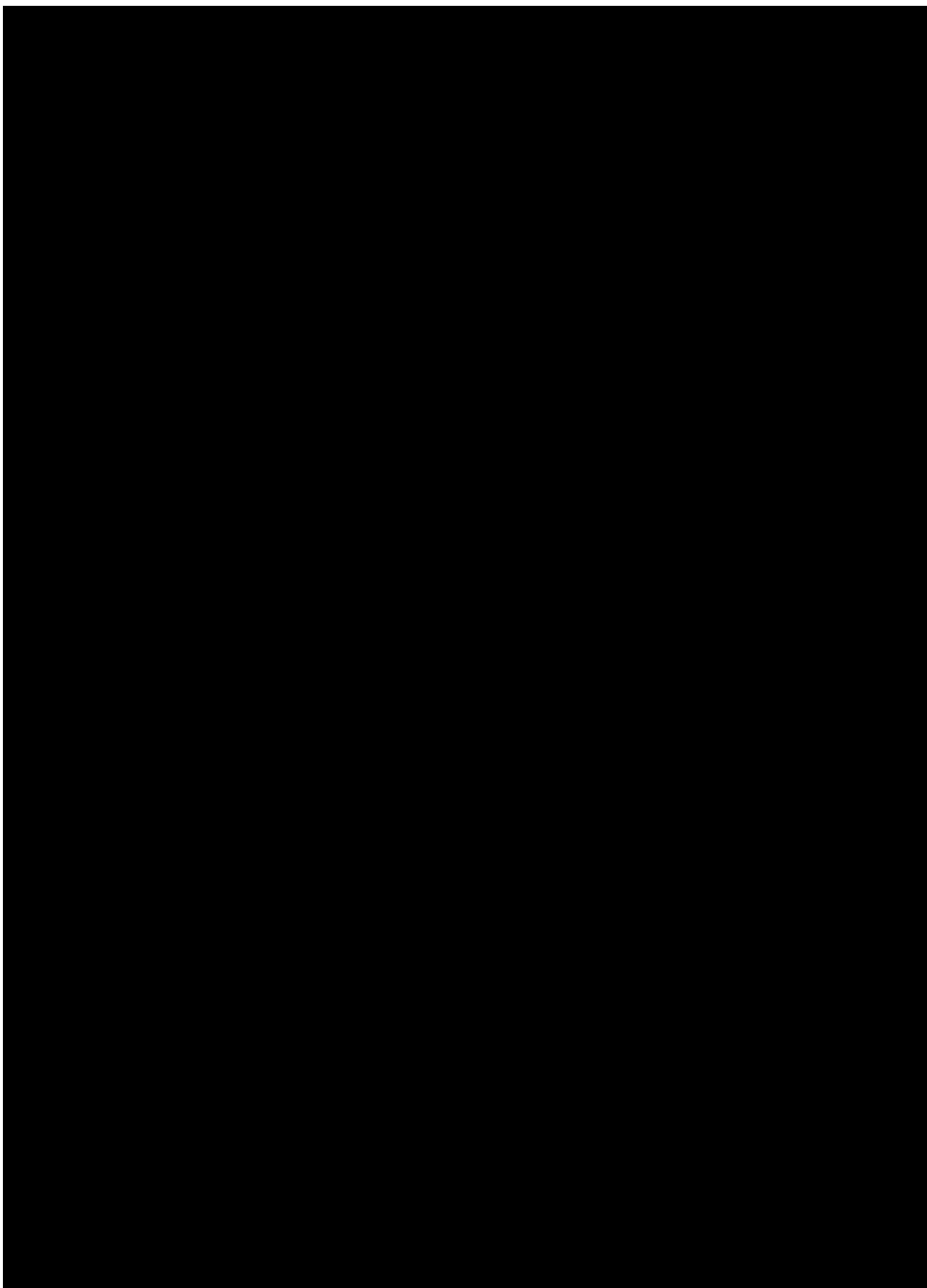
- Organizace, které k řešení přistupují (organizace, která řešení požaduje (např. z důvodu agendy), SPCSS jako poskytovatel housingu/hostingu, dodavatel, pokud je v řešení zainteresován)
- Role v organizacích, které k řešení přistupují
- Způsob přístupu k infrastruktuře (Govbone, internet)
- Aplikaci/aplikace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

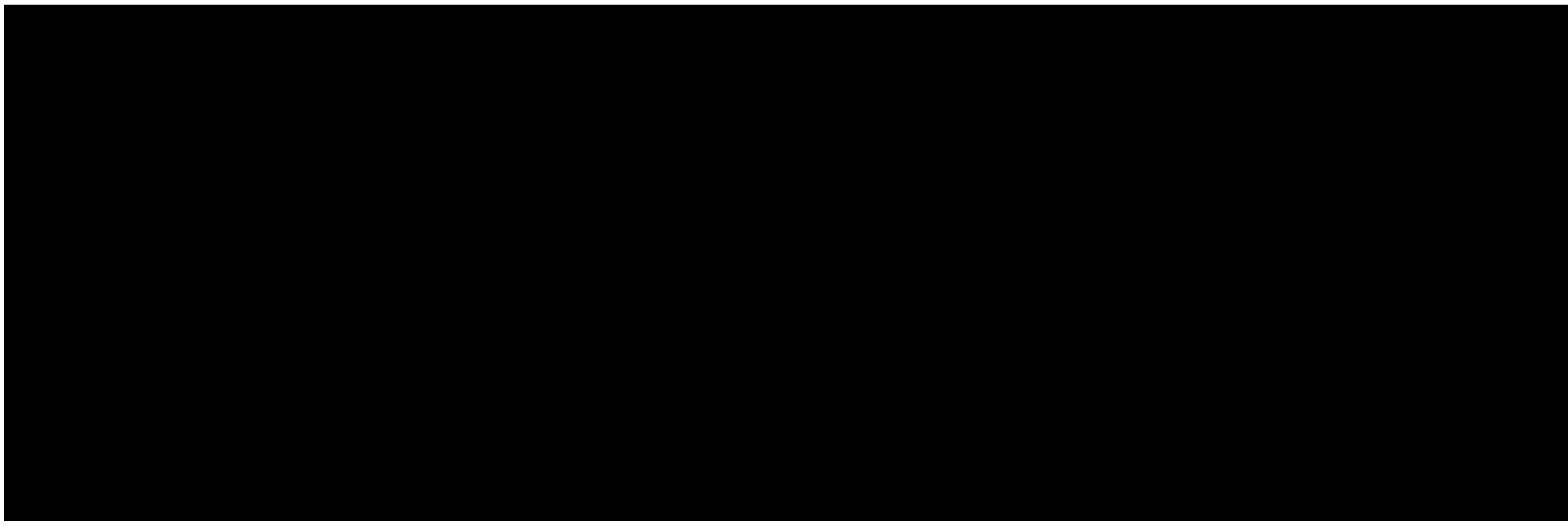
Kapitola popíše platformu na které bude služba poskytována. Pokud se jedná o ISVS, lze vybrat jen platformu, která je zapsaná v katalogu CC pro příslušnou Bezpečnostní úroveň.

3.2.1.1 MS Azure

Kapitola popíše HW parametry prostředí Azure. V případě že nebude toto prostředí využito zapíše se není relevantní.

3.2.1.1.1 FinOps

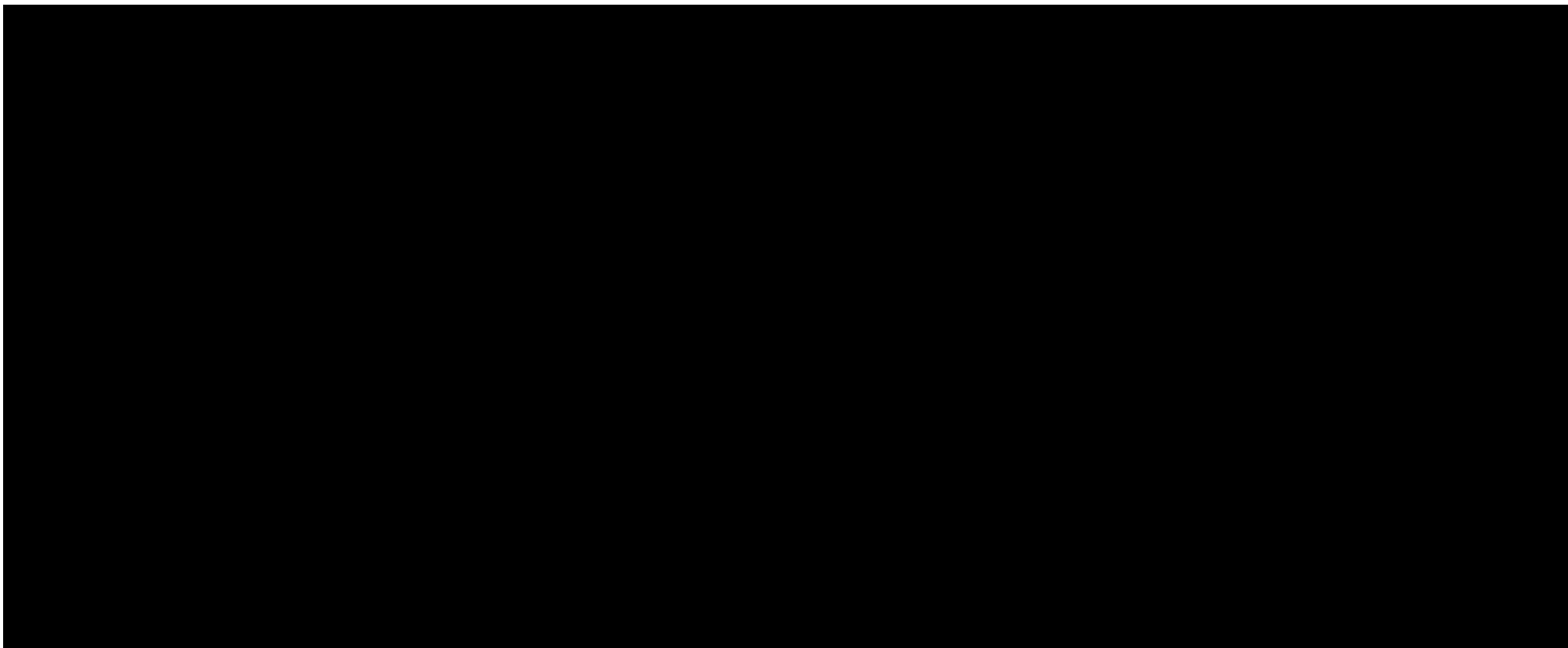
Tato kapitola je zaměřena na FinOps a na představení strategií a nejlepších praktik pro efektivní správu nákladů a zdrojů v Microsoft Azure. Jak efektivně spravovat cloudové náklady, nejen aby byly udrženy v rozumných mezích, ale také aby byly v souladu s obchodními cíli a strategiemi. FinOps není jen o snižování nákladů; je to o vytváření hodnoty, transparentnosti a o optimalizaci investic, což umožňuje rychleji reagovat na tržní změny a inovovat.



3.2.1.1.2 Poznámky

Není relevantní.

3.2.1.2 AzureStack Hub



3.2.1.3 VMWare

Kapitola popisuje HW parametry prostředí VMWare. V případě že nebude toto prostředí využito zapíše se není relevantní.

3.2.1.4 Power

Kapitola popíše HW parametry prostředí Power. V případě že nebude toto prostředí využito zapíše se není relevantní.

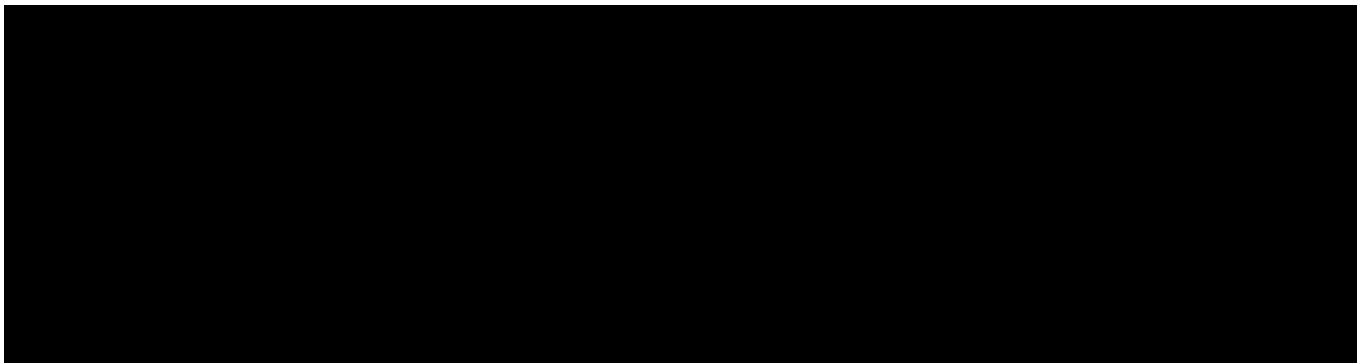
3.2.1.5 Google cloud

Kapitola popíše HW parametry prostředí Google cloud. V případě že nebude toto prostředí využito zapíše se není relevantní.

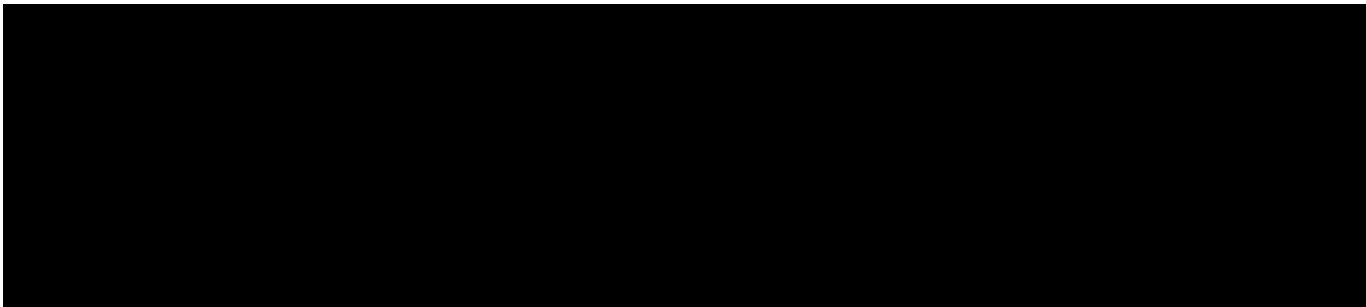
3.2.2 Storage

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

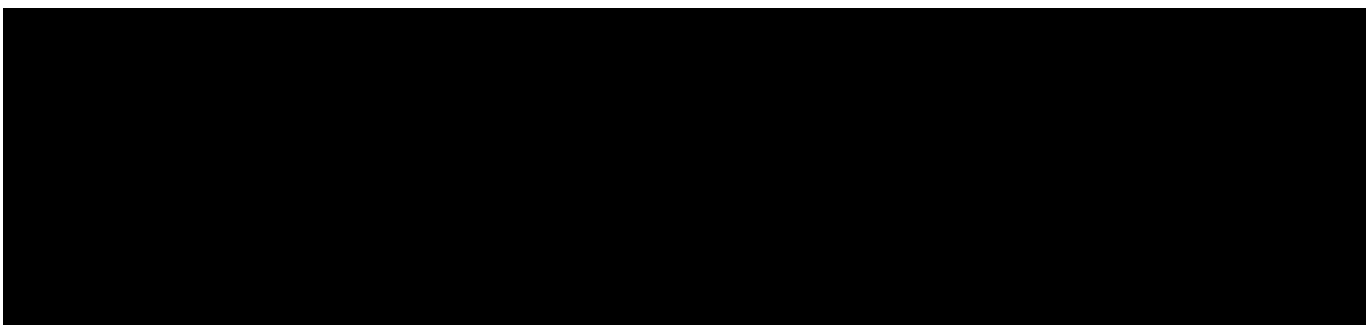
3.2.2.1 MS Azure



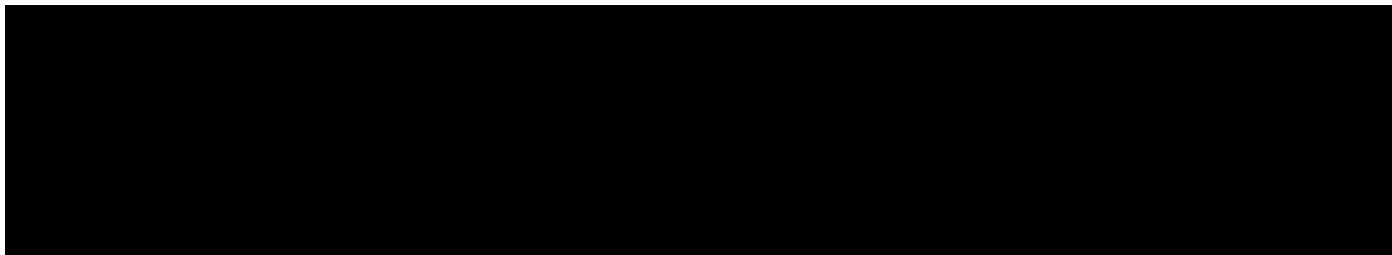
3.2.2.2 MS AzureStack Hub



3.2.2.3 VM Ware



3.2.2.4 Power



3.2.2.5 Google cloud

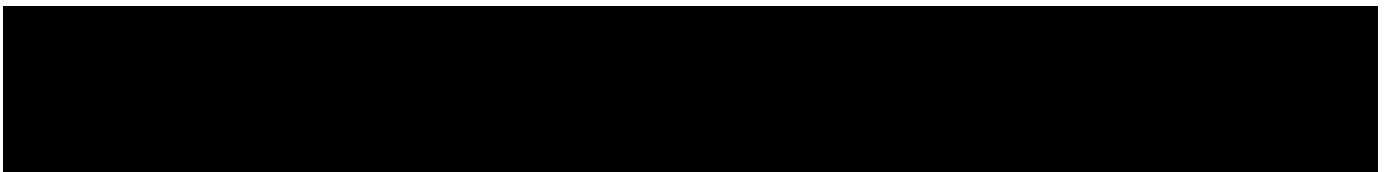


3.2.3 Databáze

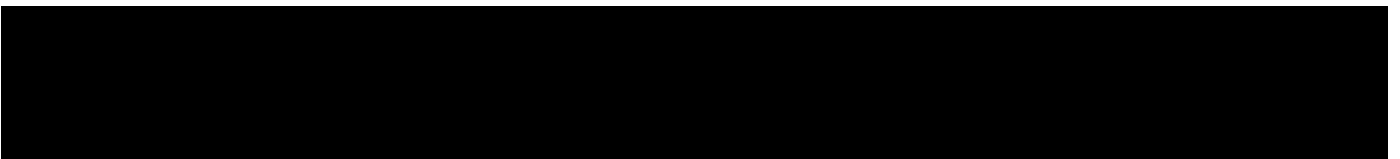
Kapitola popíše požadavky zákazníka a jeho řešení na využití databází



3.2.3.1 On-Premise



3.2.3.2 Cloud (BÚ 3)



3.2.3.3 Poznámky

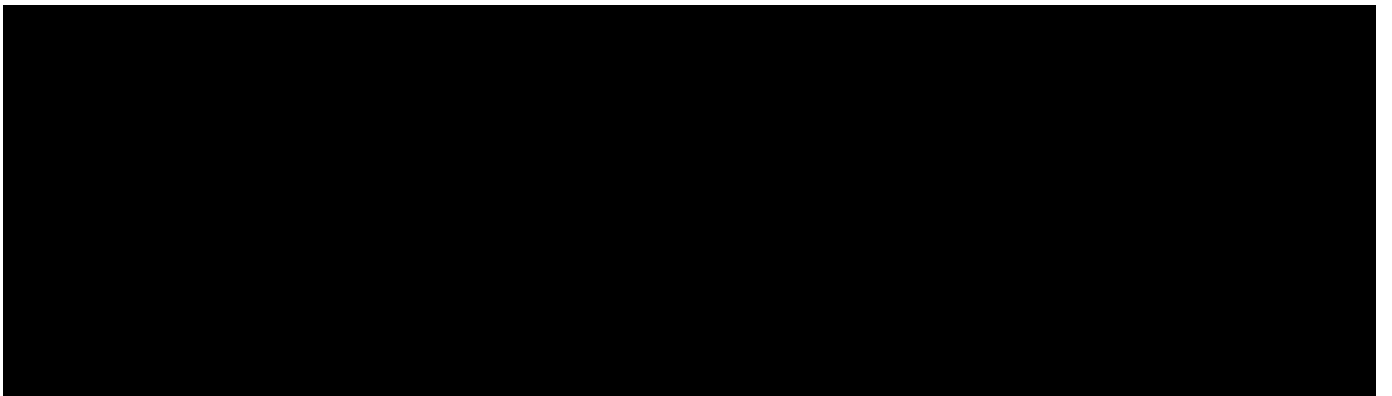
Kapitola popíše případné podrobnosti a požadavky na řešení DB.



3.2.4 Síťová platforma

3.2.4.1 FW throughput

Kapitola popíše zákazníkem celkový požadovaný throughput skrz FW SPCSS.



3.2.4.2 VPN

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

3.2.4.3 Ostatní datové okruhy

Kapitola volným textem popíše případné další datové konektivity, datové okruhy, které v rámci předmětné služby vzniknou.

3.2.5 HSM / KeyVault

Kapitola popíše požadavky systému na použití HSM v on-premise, případně KeyVaultu v cloudu.

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-premise i Cloud.*

3.2.6.2 Cloud

3.2.6.3 Poznámky

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

3.2.7 Logování

Kapitola popíše požadavky zákazníka na logování.

3.2.7.2 Cloud

3.2.7.3 Poznámky

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

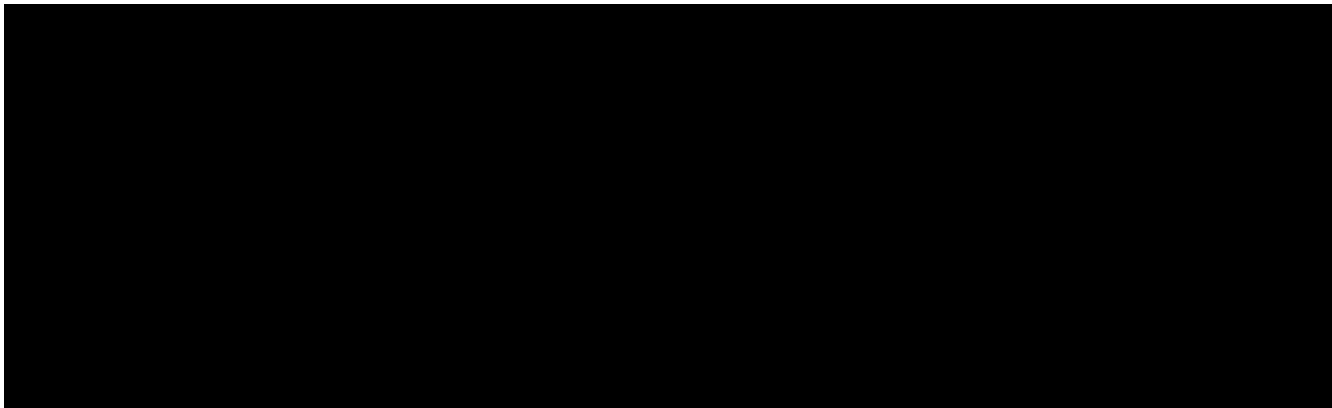
3.2.8 Zálohování

Kapitola popíše způsob, četnost a retenci záloh požadovaných systémem/dodavatelem aplikace

Typ zálohy – snapshot, nebo souborová záloha

Četnost záloh – jak často bude záloha vykonávána

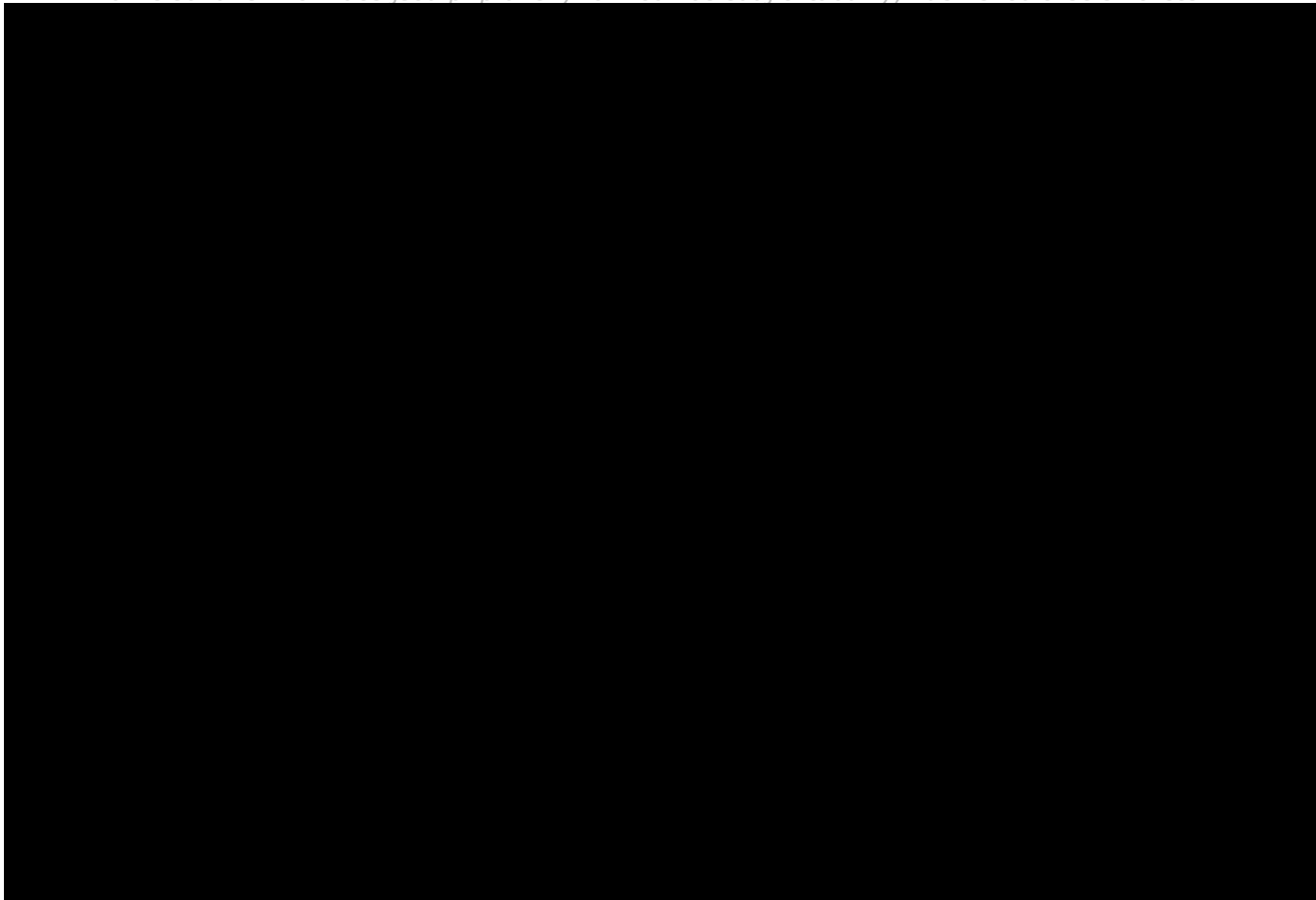
Retence záloh – jak dlouhou bude záloha uchována, než se smaže. Údaj je ve dnech

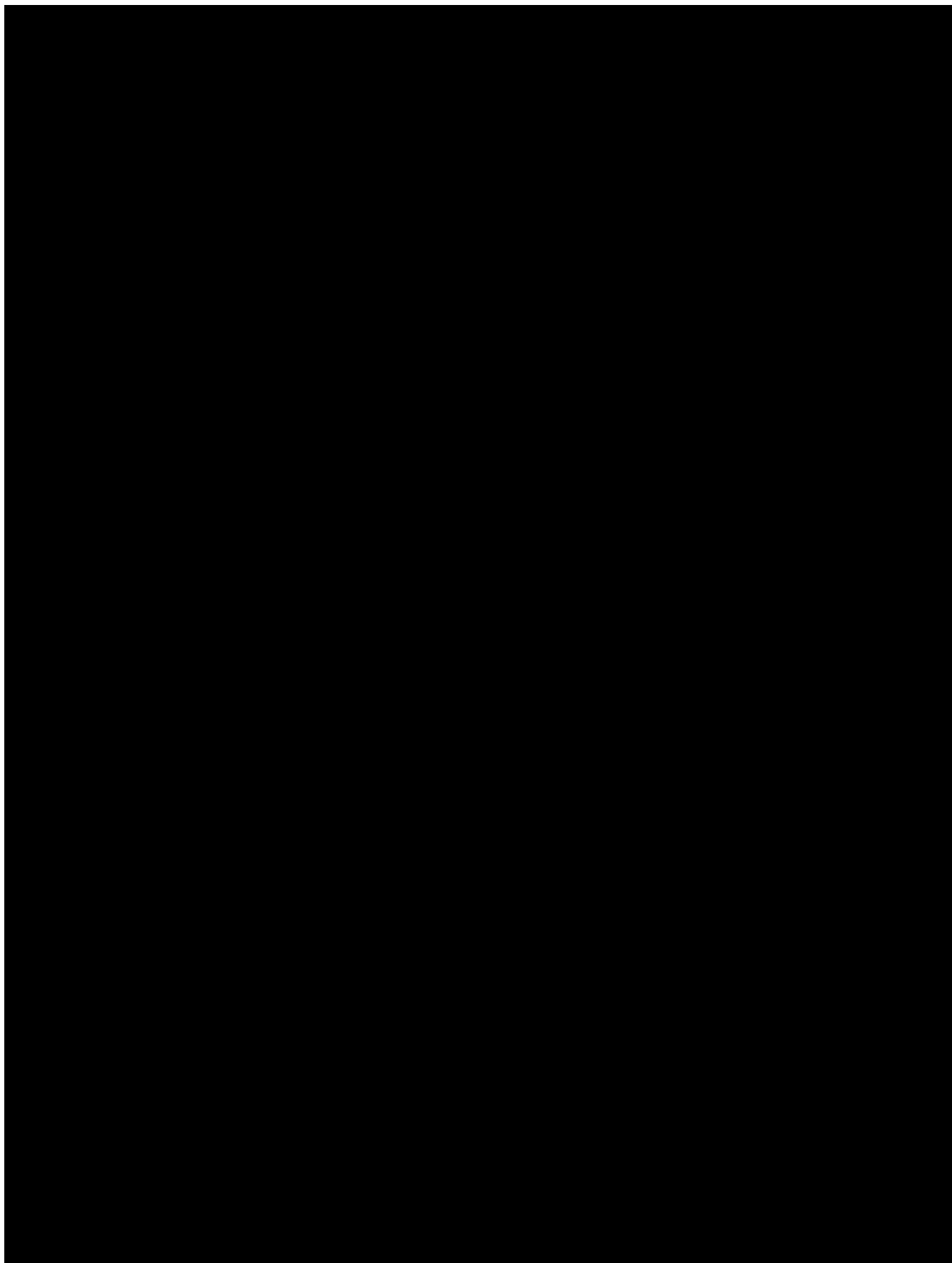


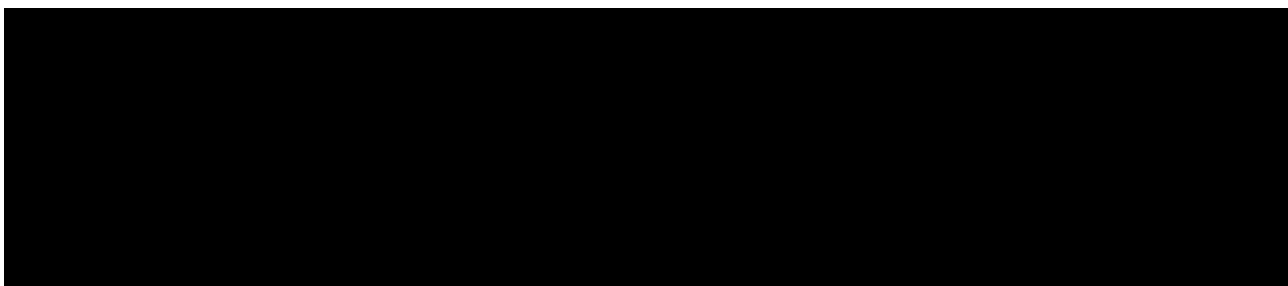
4 Bezpečnostní požadavky

Kapitola popíše požadavky zákazníka na bezpečnost, bezpečnostní a provozní monitoring.

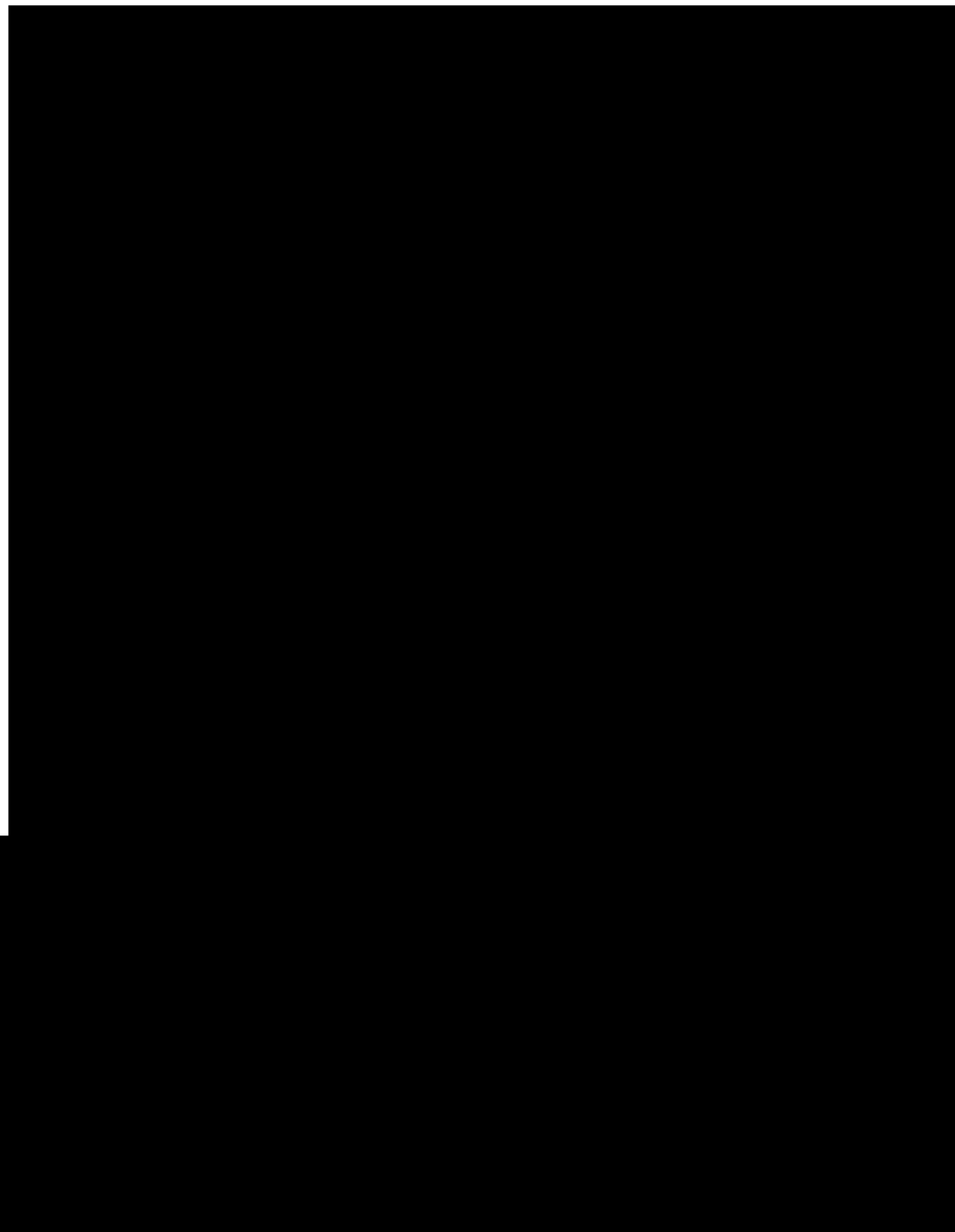
Primárně sbírané informace jsou připraveny formou následující tabulky, kde nehodící se škrtněte.







5 Podpisová doložka



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.	