Seznam nezbytných programů pro provoz a životní cyklus Aplikací

Verze: 1.0
Klasifikace: Partner Confidential
Vlastník: MAZEVAULT s.r.o.
Datum účinnosti smlouvy („Datum účinnosti“): 01.04.2026
Cyklus revize: Roční
Schválil: Jednatel MV

Tento dokument tvoří nedílnou součást smluvní dokumentace mezi Poskytovatelem a Zákazníkem ve smyslu Licenčních podmínek užívání Aplikací MV (dále jen „Licenční podmínky"). V případě rozporu mezi tímto dokumentem a Licenčními podmínkami mají přednost v otázkách technické podpory a životního cyklu ustanovení tohoto dokumentu; v ostatních věcech mají přednost Licenční podmínky.

---

1. Úvod

MAZEVAULT s.r.o. (dále jen „MV") je autorem a vlastníkem Aplikací MazeVault — podnikové platformy pro centralizovanou správu šifrovacích klíčů, digitálních certifikátů, hesel a dalších tajných údajů (KMS a PKI infrastruktura). MV vydává Aplikace, provádí jejich vývoj, vydává aktualizace a bezpečnostní opravy a určuje pravidla životního cyklu produktu.

Aplikace jsou zákazníkům (dále jen „Zákazník") poskytovány prostřednictvím Partnera — podnikatele, který od MV získal licenci a dále je poskytuje Zákazníkům, zajišťuje nasazení Aplikace a je primárním kontaktním místem pro technickou podporu (dále jen „Partner"). MV odpovídá ve vztahu k Partnerovi; ve vztahu k Zákazníkovi odpovídá za provoz, údržbu a bezpečnost Aplikace výhradně Partner, není-li v příslušné smlouvě výslovně sjednáno jinak.

Zákazník instaluje a provozuje Aplikace **na vlastní infrastruktuře** nebo v cloudovém prostředí Partnera. MV v žádném případě nezajišťuje ani neprovozuje infrastrukturu Zákazníka. Zákazník nese veškeré náklady na provoz, zabezpečení, infrastrukturu a jejich rozšíření ve všech zvolených provozních režimech.

Pro účely Smlouvy jsou Aplikace poskytované Poskytovatelem Zákazníkovi vymezeny v následujících licenčních variantách:

1. MazeVault PoC – časově omezená evaluační nebo pilotní licence pro ověření řešení;

2. MazeVault Small Business – standardní placená licence pro menší zákazníky;
3. MazeVault Enterprise – plná podniková licence.

Tento dokument (dále jen „Politika") definuje:

1. závazky MV v oblasti vydávání aktualizací, bezpečnostních záplat a oznamování životního cyklu;
2. odpovědnosti Zákazníka při provozu Aplikací;
3. bezpečnostní závazky specifické pro bezpečnostně kritický charakter Aplikací: kryptografické standardy, řešení bezpečnostních incidentů, hlášení zranitelností, bezpečnostní doporučení.

---

2. Rozsah dokumentu

2.1 Aplikace v rozsahu

Tato Politika se vztahuje na následující součásti Aplikací MazeVault:

Součást	**Popis**
Backend API MazeVault	Správa tajných klíčů, životní cyklus certifikátů, RBAC, auditní logování
Webové rozhraní MazeVault	Správcovské rozhraní v prohlížeči
Agent MazeVault	Lehký koncový agent pro distribuci tajných klíčů a certifikátů
Gateway MazeVault	Vstupní a směrovací vrstva
OCSP Responder MazeVault	Služba ověřování platnosti certifikátů
CLI MazeVault	Rozhraní příkazové řádky pro správu a automatizaci
Helm charty MazeVault	Manifesty nasazení pro Kubernetes
Terraform provider MazeVault	Integrace Infrastructure-as-Code
Licenční server MazeVault	Validace a vynucování licencí
Dokumentace	Zákaznická dokumentace

2.2 Mimo rozsah

Tato Politika se nevztahuje na:

4. infrastrukturu Zákazníka (hardware, OS, síťová infrastruktura, Kubernetes cluster, databáze, zálohy, monitoring, fyzická bezpečnost) — za tyto oblasti odpovídá výhradně Zákazník, není-li výslovně sjednáno jinak;
5. infrastrukturu Partnera (pokud Zákazník využívá cloudový provoz Partnera) — za tuto odpovídá Partner;

6. aplikační kód Zákazníka nebo integrační logiku vytvořenou Zákazníkem nad API Aplikací;
7. služby třetích stran integrované s Aplikacemi (Azure Entra ID, Azure Key Vault, AWS Secrets Manager, HashiCorp Vault, externí CA) — tyto se řídí podmínkami příslušných třetích stran;
8. zakázkový vývoj a profesionální služby — řídí se samostatnou smlouvou o dílo;
9. školení a certifikace — řídí se samostatnou smlouvou.

2.3 Smluvní strany a model podpory

Podpora funguje v následujícím modelu:

Vrstva	**Subjekt**	**Závazek**
Vývojová (upstream)	MV	Vydávání aktualizací, bezpečnostních záplat, bezpečnostních doporučení; definice životního cyklu verzí
Distribuční	Partner	Primární podpora Zákazníkovi; nasazení a konfigurace; eskalace vůči MV
Provozní	Zákazník	Provoz infrastruktury; aplikace aktualizací; zabezpečení prostředí; zálohování

2.4 Podporované modely nasazení

Model nasazení	**Provozovatel infrastruktury**	**Pokrytí Aplikací**
On-premise Docker Compose	Zákazník	Aplikační vrstva
On-premise Kubernetes / Azure AKS	Zákazník	Aplikační vrstva
Cloud Partnera	Partner	Aplikační vrstva + infrastruktura dle smlouvy s Partnerem
Hybridní (on-premise Gateway + cloudová řídicí rovina)	Zákazník / dle konfigurace	Aplikační vrstva dle komponenty

---

3. Definice

Pojmy s velkým počátečním písmenem mají v tomto dokumentu stejný význam jako v Licenčních podmínkách, není-li níže definováno jinak.

Pojem	Definice
MV nebo Poskytovatel	MAZEVAULT s.r.o., IČO 24517194, autor a vlastník Aplikací
Partner	Podnikatel oprávněný od MV nabízet a prodávat Zákazníkům Licence; primární podpora Zákazníkovi
Zákazník	Podnikatel, který uzavřel smlouvu s Partnerem a užívá Aplikace na základě Licence
Uživatel	Osoba na straně Zákazníka oprávněná Aplikaci užívat
Aplikace	Počítačové programy MazeVault ve všech verzích, modulech, aktualizacích a doplňcích
Licence	Nevýhradní, časově omezené a nepřevoditelné oprávnění k užívání Aplikací udělené Zákazníkovi
Předplatné	Časové období, po které má Zákazník na základě Licence umožněn přístup k Aplikaci
Aktualizace a opravy	Opravy chyb, bezpečnostní záplaty, úpravy nebo vylepšení vydávané MV
Zákaznická data	Veškerá data, která Zákazník nebo jeho Uživatelé vloží do Aplikace nebo zpracují jejím prostřednictvím
Bezpečnostní aktiva	Digitální certifikáty, privátní klíče, šifrovací klíče, API klíče, přístupové údaje, hesla, tokeny, secrets, kryptografické materiály a konfigurační údaje
Bezpečnostní incident	Jakákoli událost vedoucí nebo způsobilá vést k narušení důvěrnosti, integrity nebo dostupnosti Aplikace nebo Bezpečnostních aktiv
Podporovaná konfigurace	Konfigurace Aplikace provozovaná v souladu s dokumentací MV, doporučenými verzemi OS, databází, middleware a dalších komponent
Incident	Neplánované přerušení nebo degradace funkcionality Aplikace nebo Bezpečnostní incident
CVE	Common Vulnerabilities and Exposures —

Pojem	Definice
	standardizovaný identifikátor veřejně známých zranitelností
CVSS	Common Vulnerability Scoring System — rámec pro hodnocení závažnosti zranitelností
Kritická zranitelnost	Zranitelnost se skóre CVSS ≥ 9,0 nebo jakákoli zranitelnost umožňující neoprávněný přístup k Bezpečnostním aktivům bez ohledu na skóre CVSS
Podporovaná verze	Verze Aplikace aktivně přijímající údržbu a bezpečnostní záplaty dle tohoto dokumentu
KPP	Konec prodeje (End of Sale) — verze se již nenabízí novým Zákazníkům
KÚ	Konec údržby (End of Maintenance) — pro verzi se nevydávají žádné aktualizace údržby
KPod	Konec podpory (End of Support) — pro verzi nejsou vydávány žádné záplaty ani přijímány požadavky na podporu
KŽC	Konec životního cyklu (End of Life) — verze nepřijímá žádné aktualizace
Pracovní hodiny	Pondělí – pátek, 08:00 – 16:00 SEČ, s výjimkou českých státních svátků
Rozšířené hodiny	Pondělí – pátek, 07:00 – 18:00 SEČ
Pohotovostní provoz	24/7, výhradně pro kritické incidenty P1
Okno údržby	Plánované období přípustného přerušení provozu z důvodu aktualizace nebo údržby Aplikace
Bezpečnostní doporučení	Formální oznámení MV popisující potvrzenou zranitelnost a dostupné řešení
SBOM	Software Bill of Materials — inventář všech softwarových komponent a závislostí

---

4. Technické požadavky na provoz

4.1 Minimální technické požadavky na provoz:

Komponenta	CPU	RAM	HDD
API server	2 cores	4 GB	20 GB SSD
PostgreSQL	2 cores	4 GB	50 GB SSD
Redis	1 core	1 GB	5 GB SSD
Webové rozhraní	1 core	512 MB	1 GB SSD

OCSP responder	1 core	512 MB	1 GB SSD
Agent	1 core	128 MB	1 GB SSD
Dokumentace	1 core	512 MB	1 GB SSD

4.2 Doporučené produkční technické požadavky:

Komponenta	**CPU**	**RAM**	**HDD**
API server	4+ cores	8+ GB	50 GB SSD
PostgreSQL	4+ cores	16+ GB	200+ GB SSD
Redis	4+ cores	4+ GB	10 GB SSD
Webové rozhraní	2 cores	2 GB	5 GB SSD
OCSP responder	2 cores	1 GB	5 GB SSD
Agent	1 core	128 MB	5 GB SSD
Dokumentace	1 core	512 MB	1 GB SSD

4.3 Síťové požadavky

Externí porty:

1. TCP 443 pro HTTPS
2. TCP 80 pro redirect na HTTPS

Interní porty, které **nesmí** být veřejně vystaveny do Internetu bez řádného zabezpečení firewallem nebo jiným adekvátním způsobem dle Licenčních podmínek:

1. TCP 8080 pro API
2. TCP 8081 pro OCSP
3. TCP 5432 pro PostgreSQL
4. TCP 6379 pro Redis

Odchozí komunikace dle používaných funkcí:

1. HTTPS 443 na MazeVault License Server – https://license.mazevault.com
2. HTTPS 443 na Azure Entra ID při použití SSO
3. HTTPS 443 na Azure Key Vault nebo jiné externí vaulty při použití integrací
4. HTTPS 443 na externí CA při použití externích certifikačních autorit
5. HTTPS 443 na MazeVault agenta / proxy při použití v hybridním režimu infrastruktury mimo LAN
6. UDP 123 na NTP server pro časovou synchronizaci
7. TCP 1433, 1521, 5432 a další na různé databázové platformy při integracích na databáze pro správu a rotaci Secrets a Certifikátů

8. jakékoliv custom porty zvolené Zákazníkem při integraci komponent na systém MazeVault (JIRA, Teams, e-mail, SIEM, ELK, Slack a další integrace existující či nově přidané)

4.4 Seznam nezbytných programů pro provoz Aplikací

Nezbytné programy a služby pro standardní provoz Aplikací:

1. PostgreSQL 15+;
2. Redis 7.x+;
3. Docker Engine 24+ nebo Podman;
4. Docker Compose 2.20+ nebo podman-compose;
5. Nginx 1.24+ nebo jiný reverse proxy či ingress ekvivalent;
6. webový prohlížeč v podporované verzi.

Nezbytné programy a služby pro Kubernetes variantu provozu:

1. Kubernetes 1.28+;
2. Helm 3.12+;
3. kubectl 1.28+;
4. Azure CLI 2.50+;
5. External Secrets Operator a Workload Identity při použití customer Azure modelu s Azure Key Vault.

Podmíněně nezbytné programy nebo služby při použití odpovídajících funkcí:

1. Azure Entra ID při použití SSO;
2. Azure Key Vault, AWS Secrets Manager nebo HashiCorp Vault při použití externí správy tajemství nebo klíčů;
3. externí CA systémy při použití vydávání certifikátů mimo interní CA;
4. HSM při nasazení HSM funkcí.

Zákazník bere na vědomí, že k řádnému užívání Aplikací mohou být vedle Licence Poskytovatele nezbytné také licence nebo oprávnění k programům a službám třetích stran, které se řídí podmínkami příslušných třetích stran.

---

5. Podporované licence

Technická podpora se poskytuje Zákazníkům s aktivní a zaplacenou Licencí. Rozsah podpory se odvíjí od licenční varianty:

Licence	**Úroveň podpory**	**Pracovní hodiny**	**Pohotovostní provoz (P1)**
MazeVault PoC	Komunitní	Samoobslužná	Ne

Licence	Úroveň podpory	Pracovní hodiny	Pohotovostní provoz (P1)
		dokumentace	
MazeVault Small Business	Standardní	Pracovní hodiny	Ne
MazeVault Enterprise	Rozšířená	Rozšířené hodiny	Ne
Enterprise + prémiový doplněk	Prémiová	24/7	Ano

Licence PoC: Poskytuje se výhradně pro evaluaci, maximálně po dobu 3 měsíců, bezplatně. Nevztahuje se na ni žádný závazek SLA. Bezpečnostní záplaty jsou Zákazníkovi PoC oznamovány prostřednictvím Bezpečnostních doporučení.

Zánik Předplatného: Ukončením nebo uplynutím Předplatného zanikají závazky technické podpory. Bezpečnostní doporučení jsou nadále vydávány v rámci okna životního cyklu dané verze.

---

6. Podporované platformy

Aplikace jsou podporovány na následujících platformách při nasazení v souladu s dokumentací MV:

Tato sekce definuje **matici podpory softwaru MazeVault** — tj. pro které platformy MV vydává záplaty a poskytuje technickou podporu. Smluvní **minimální technické požadavky pro Zákazníka:**

6.1 Operační systémy (on-premise)

OS	Verze	Stav
Rocky Linux	9.x	Podporováno
RHEL	9.x	Podporováno
Rocky Linux	8.x	Podporováno (pouze bezpečnostní aktualizace)
RHEL	8.x	Podporováno (pouze bezpečnostní aktualizace)
Ubuntu	22.04 LTS	Podporováno
Ubuntu	20.04 LTS	Podporováno (pouze bezpečnostní aktualizace)
Jiný Linux	—	Nejlepší úsilí; bez záruky
Windows Server	—	Nepodporováno
macOS	—	Nepodporováno (pouze vývojové prostředí / CLI)

6.2 Kontejnery a orchestrace

Platforma	Verze	Stav
Docker Engine	24.x, 25.x, 26.x	Podporováno
Docker Compose	2.20+	Podporováno
Podman	4.x	Nejlepší úsilí
Kubernetes	1.28 – 1.32	Podporováno
Azure AKS	Aktuální – N-2	Podporováno
Helm	3.12+	Podporováno
Nginx nebo funkčně ekvivalentní reverse proxy řešení	1.24+	Podporováno
kubectl	1.28+	Podporováno
Azure CLI	2.50+	Podporováno
Terraform	1.5+	Podporováno

6.3 Databáze

Databáze	Verze	Stav
PostgreSQL	15, 16, 17	Podporováno
PostgreSQL	14	Podporováno (pouze bezpečnostní aktualizace)
SQLite	3.x	Pouze PoC / dev; nepodporováno v produkci

6.4 Cloudové integrace

Poskytovatel	Služba	Stav
Microsoft Azure	Key Vault, Entra ID	Integrace podporována
AWS	Secrets Manager	Integrace podporována
HashiCorp	Vault	Integrace podporována
On-premise	HSM (PKCS#11)	Podporováno pro Enterprise

6.5 Webové prohlížeče

Prohlížeč	Verze	Stav
Google Chrome	100+	Podporováno
Mozilla Firefox	100+	Podporováno
Microsoft Edge	100+	Podporováno
Safari	16+	Podporováno

Verze označené jako „pouze bezpečnostní aktualizace" jsou technicky podporovány softwarem MazeVault, avšak mohou nesplňovat stanovené smluvní minimum Rocky Linux / RHEL 9+,

PostgreSQL 15+ a Redis 7.x+. Zákazníci provozující starší verze nesplňují minimální technické požadavky Smlouvy; Poskytovatel se může řídit podmínkami příslušné smlouvy.

---

7. Podporované konfigurace

Podporovanými konfiguracemi ve smyslu Licenčních podmínek jsou:

Konfigurace	Infrastruktura	Podrobnosti
On-premise Docker Compose	Zákazník	Jednouzlový; Small Business; doporučeno pro neprodukční prostředí nebo menší instalace
On-premise Kubernetes HA	Zákazník	Multi-replika; PostgreSQL 15+; Redis s persistencí; Nginx/Traefik ingress
Azure AKS	Zákazník nebo Partner	Kubernetes na Azure; cert-manager; Workload Identity
Hybridní Gateway	Zákazník	On-premise Gateway + cloudová řídicí rovina Zákazníka; mTLS
Azure Workload Identity	Zákazník	Managed Identity pro přístup k Azure Key Vault bez statických přihlašovacích údajů
Integrace s externí CA	Zákazník	ACME, SCEP, Step CA, interní CA
SSO přes Entra ID (OIDC)	Zákazník	Federace s Azure Active Directory / Entra ID
SSO přes SAML 2.0	Zákazník	Libovolný IdP kompatibilní se SAML 2.0
SIEM integrace	Zákazník	Elasticsearch, Splunk HEC, Microsoft Sentinel, IBM QRadar, Syslog RFC 5424
HSM ochrana klíčů	Zákazník	PKCS#11 HSM pro kořenovou CA; Enterprise

---

8. Nepodporované konfigurace

Problémy vzniklé z Nepodporované konfigurace nejsou způsobilé pro záruky ani závazky SLA. Provoz Aplikace v Nepodporované konfiguraci může být posouzen jako podstatné porušení Smlouvy:

Nepodporovaná konfigurace	**Důvod**
Produkční provoz na SQLite	Nevhodné pro HA; riziko ztráty dat
Přímé vystavení Aplikace do veřejné sítě Internet bez reverse proxy / firewallu	Podstatné porušení Licenčních podmínek; bezpečnostní riziko
Verze po Konci podpory	Žádné bezpečnostní záplaty; nesoulad s bezpečnostními povinnostmi Zákazníka
Vlastní záplaty nebo modifikace binárních souborů Aplikací	Porušení Licenčních podmínek; ruší záruky
Sdílení databázové instance PostgreSQL s nedůvěryhodnými workloady	Bezpečnostní požadavek na izolaci dat
Zakázání TLS pro interní komunikaci služeb	Porušení minimálního bezpečnostního postoje; netestováno
Zakázání auditního logování v produkci	Porušení Licenčních podmínek; nesoulad s regulatorními požadavky
Spouštění Agenta jako root	Zbytečná eskalace oprávnění; explicitně nedoporučováno
Nasazení bez síťové izolace v Kubernetes	Bezpečnostní požadavek platformy
SHA-1 nebo MD5 pro podepisování certifikátů	Kryptograficky prolomeno; platforma odmítá
Obcházení licenčních nebo bezpečnostních mechanismů Aplikace	Podstatné porušení Licenčních podmínek
Penetrační testy bez předchozího písemného souhlasu	Porušení Licenčních podmínek