TRULY AGENTIC (INDEPENDENT ENGINEERING PRACTICE — ANIL PERVAIZ)

Compliance & Security Report

Comprehensive overview of security controls, compliance frameworks, and data protection practices.

November 24, 2026

CONFIDENTIAL

https://trulyagentic.io

security@trulyagentic.io

Compliance Frameworks

Framework	Status	Description
OWASP Top 10 for Agentic AI (2026)	IN PROGRESS	Runtime controls mapped directly to ASI01–ASI06 (Goal Hijack, Tool Misuse, Privilege Abuse, MCP Poisoning/Rug Pulls, Unexpected Execution, Context Poisoning) in our open-source Governance Kit v0.1.0 (synthetic lab benchmarked).
SOC 2 Type II	IN PROGRESS	Pre-audit technical controls mapped to AICPA Trust Services Criteria (Security, Availability, Confidentiality). Not currently SOC 2 certified — formal third-party CPA examination planned alongside enterprise procurement.
ISO/IEC 27001:2022	IN PROGRESS	BYOC isolation, IAM separation, KMS custody, and append-only audit controls aligned to Annex A domains. Not currently ISO 27001 certified — source and Terraform IaC transparency provided under Mutual NDA.
CSA STAR Level 1 (CAIQ-Lite)	IN PROGRESS	Cloud Security Alliance CAIQ-Lite self-assessment tailored for single-tenant BYOC deployments published transparently on this Trust Center; formal CSA registry filing planned.
UAE PDPL (Federal Decree-Law No. 45/2021)	IN PROGRESS	Bring-Your-Own-Cloud (BYOC) execution keeps operational records inside the client UAE or regional cloud VPC, minimizing cross-border transfers. Baseline DPA template available under Mutual NDA.
Dubai DESC ISR v3 Alignment	IN PROGRESS	Workload identity isolation, segregation of read/propose/write duties, customer-managed KMS keys, and tamper-evident logging aligned to Dubai Electronic Security Center ISR domains.
GDPR / UK GDPR	IN PROGRESS	Zero advertising cookies on public web properties, EU-hosted transactional email (Ireland eu-west-1) and privacy-first analytics (EU Frankfurt), and zero multi-tenant SaaS customer storage.
DORA / CMMC L2 Alignment	PLANNED	BYOC delivery preserves customer ICT portability, zero vendor lock-in, write-only WORM audit sinks, and customer-owned Git repository custody.

Agentic AI & MCP Governance

5/5 controls implemented

Control	Status	Description
Five Deterministic Runtime Controls (Open-Source Verified)	IMPLEMENTED	Every tool invocation passes sequentially through Control 1 (Service Identity), OWASP ASI01/ASI04 Scanner, Control 2 (Read/Propose/Write Separation), Control 3 (Named Human Sign-Off), Control 4 (Budget Caps & Kill Switch), and Control 5 (Fail-Closed Ledger).
MCP Tool Poisoning & SHA-256 Rug-Pull Detection (ASI04)	IMPLEMENTED	scanMcpToolDefinition inspects tool metadata for <IMPORTANT> or cross-tool shadowing directives and verifies canonical JSON SHA-256 hashes against pinned manifest baselines prior to runtime dispatch.
Indirect Prompt Injection Payload Scanner (ASI01)	IMPLEMENTED	scanUntrustedPayload blocks HTML comment injections, role delimiter overrides, and zero-width obfuscation characters in incoming invoices, emails, and CRM payloads before policy evaluation.
Fail-Closed "No Log, No Action" Audit Choke-Point	IMPLEMENTED	GovernanceGateway commits a SHA-256 hash-chained pre_execution row before calling any downstream ERP, CRM, or cloud API. PostgreSQL triggers block UPDATE/DELETE and log outages trigger hard aborts.
Instant Lease Kill Switch & Workflow Budget Caps	IMPLEMENTED	Pre-flight spend reservations bound execution cost per workflow; AgentRegistry.suspend immediately halts active agent leases and records an immutable kill_switch audit event.

Data Protection

4/4 controls implemented

Control	Status	Description
Zero Multi-Tenant Customer Data Egress (BYOC)	IMPLEMENTED	Truly Agentic operates no multi-tenant SaaS holding customer invoices, ERP rows, OAuth refresh tokens, or operational audit trails. All runtime state lives inside customer-owned AWS, GCP, or Azure subscriptions.
Private Zero-Retention Model Inference	IMPLEMENTED	Reference deployments connect to private VPC model endpoints (AWS Bedrock PrivateLink, GCP Vertex AI Private Service Connect, Azure OpenAI Private Endpoint) with model training disabled.
Customer-Managed Encryption & Secret Custody	IMPLEMENTED	AWS KMS (rotation enabled), GCP Cloud KMS, and Azure Key Vault keep root encryption keys under customer IAM control. Short-lived secrets inject via native Secrets Manager / Key Vault.
Immutable WORM Audit Retention Sinks	IMPLEMENTED	Terraform starters configure AWS S3 Object Lock and GCP Cloud Storage bucket retention lock with write-only (s3:PutObject / storage.objectCreator) IAM boundaries.

Access Control

3/3 controls implemented

Control	Status	Description
Workload Service Account Enforcement	IMPLEMENTED	AgentRegistry (isValidServiceAccount) permits only scoped service accounts (svc-agent-*) with explicit tool allowlists and rejects personal email identities or shared super-admin credentials.
Named Individual Slack/Teams Approval Gate	IMPLEMENTED	Irreversible write actions pause for HMAC-SHA256 verified approval bound to exact (agentId, toolName, inputSha256, idempotencyKey) from a named individual user ID (usr_*), neutralizing duplicate-click replays.
Zero Standing Contractor Access Post-Handover	IMPLEMENTED	Weeks 1–2 run read-only; Weeks 3–4 run shadow mode without ERP mutations; temporary onboarding SSO/VPN leases expire automatically upon engagement handover.

Infrastructure Security

3/3 controls implemented

Control	Status	Description
Private VPC Subnets & Loopback Docker Binding	IMPLEMENTED	Production Terraform templates deploy compute inside private subnets without public ingress. Self-hosted Docker Compose binds PostgreSQL (5432) and Portkey OSS gateway (8787) strictly to 127.0.0.1.
Edge TLS 1.2+, WAF & Email Authentication	IMPLEMENTED	Public web properties on trulyagentic.io and trust.trulyagentic.io enforce Cloudflare edge TLS 1.2+, HSTS, WAF, and DNS-authenticated email (SPF, DKIM, DMARC) across Zoho Mail and Resend EU.
Least-Privilege IaC Starters (Zero Wildcard Admin)	IMPLEMENTED	AWS and GCP Terraform modules grant scoped Bedrock/Vertex invoke and write-only audit object permissions with zero AdministratorAccess, iam:*, or *:* wildcard grants.

Application Security

2/3 controls implemented

Control	Status	Description
Strict TypeScript Gates & Automated Adversarial Tests	IMPLEMENTED	Governance Kit v0.1.0 enforces strict TypeScript compilation, Vitest unit tests (14/14 passing), and a 6-scenario adversarial attack-block suite on synthetic harnesses in CI.
Commit-SHA Pinned CI Actions & Frozen Lockfiles	IMPLEMENTED	GitHub Actions workflows in the public Governance Kit pin third-party actions to immutable commit SHAs with minimal read permissions and committed lockfiles (pnpm-lock.yaml / package-lock.json).
Independent Third-Party Penetration Testing	PLANNED	Continuous synthetic regression testing runs in CI, while full source and Terraform IaC are open for prospect CloudSec review under NDA. Formal independent external penetration testing is scheduled alongside enterprise contracts.

Incident Response

2/2 controls implemented

Control	Status	Description
Coordinated Vulnerability Disclosure (security.txt)	IMPLEMENTED	RFC 9116 security.txt published at https://trulyagentic.io/.well-known/security.txt routing reports to security@trulyagentic.io with a 3-business-day initial response commitment.
One-Command Agent Containment & Forensic Hash Replay	IMPLEMENTED	Compromised or misbehaving agents halt immediately via AgentRegistry.suspend and external auditors verify ledger integrity end-to-end with verifyAuditChainEntries.

Business Continuity

1/2 controls implemented

Control	Status	Description
Customer-Owned Git Custody & Zero Platform Lock-In	IMPLEMENTED	All workflows, Terraform modules, policy JSON rules, and ledger schemas live inside customer-owned Git repositories, ensuring uninterrupted operation independent of Truly Agentic.
Cross-Region Database Backup & Customer DR Alignment	PARTIAL	Persistence layers follow each customer cloud team’s snapshot schedule, WORM retention window, and regional failover policies.

Vendor Management

2/2 controls implemented

Control	Status	Description
Public Website & Comms Subprocessor Transparency	IMPLEMENTED	All SaaS vendors used for public web hosting, transactional inquiry email, corporate mail, privacy-first analytics, and scheduling are inventoried below with DPA links and geographic locations.
Zero Unannounced Subprocessor Access to Client BYOC VPCs	IMPLEMENTED	Third-party marketing, analytics, and email vendors have zero network path into customer BYOC agent runtimes, ERP data, or audit ledgers.

Governance

2/3 controls implemented

Control	Status	Description
Mutual NDA Security Package & Pre-SOC 2 Matrix	IMPLEMENTED	Architecture diagrams, CSA CAIQ-Lite / SOC 2 / ISO 27001 / UAE PDPL mappings, Terraform review guides, and baseline Mutual NDA + DPA templates are ready for prospect CloudSec and Legal review.
Mandatory Schedule B Written Testing Authorization	IMPLEMENTED	Before any active security assessment runs in a customer sandbox, written scope authorization is required under UAE Federal Decree-Law No. 34 of 2021 and applicable computer misuse laws.
Formal Third-Party GRC Audit Readiness	PARTIAL	Tracking pre-audit readiness controls continuously ahead of formal third-party SOC 2 Type I / II examination.

Subprocessors

Vendor	Purpose	Location
Cloudflare	Static edge hosting, DNS, TLS 1.2+, and WAF for public web properties only (zero customer BYOC agent workloads)	Global Edge Network
Resend	Transactional inquiry & NDA security package confirmation emails (web contact forms only)	European Union (Ireland — eu-west-1)
Zoho Mail	Direct founder & security inbox handling (founder@, hello@, security@trulyagentic.io)	Global
PostHog	Cookieless privacy-first telemetry on main marketing site (zero session replay)	European Union (Frankfurt)
Cal.com	Introductory architecture & security review call scheduling	United States / European Union
GitHub	Version control and CI execution for public Apache-2.0 Governance Kit and documentation repositories	United States

Security Questionnaire Results

Questionnaire	Total	Yes	Partial	No	N/A
CSA CAIQ-Lite (BYOC) v4.0	14	12 (86%)	1 (7%)	0 (0%)	1
OWASP Agentic AI (2026) v2026	10	10 (100%)	0 (0%)	0 (0%)	0
MVSP (BYOC Profile) v1.0	12	11 (92%)	1 (8%)	0 (0%)	0

Published Documents

Document	URL
Privacy Policy	https://trulyagentic.io/privacy
Security Policy	https://trulyagentic.io/security
subprocessors	https://trust.trulyagentic.io/#subprocessors