KARMAFLOW.AI

Platform Security Overview

Enterprise-Grade Security Architecture & Compliance Posture

Karmaflow.ai is built from the ground up with enterprise security as a foundational principle — not an afterthought. Our platform is hosted on Google Cloud infrastructure, operates within Canadian data sovereignty boundaries for all primary processing, and adheres to the rigorous internal controls required for SOC 2 Type II certification, currently in progress and targeted for completion by Q3 2026.

This document provides an overview of our infrastructure architecture, data governance practices, identity and access controls, subprocessor relationships, and organizational security posture.

COMPLIANCE & CERTIFICATION

Compliance Status at a Glance

As of 2025

SOC 2 Type II Certification Covers Security, Availability, Confidentiality trust service criteria	✓ IN PROGRESS — Target Q3 2026
Google Cloud Security Framework Infrastructure aligned to Google's enterprise security baseline	✓ ACTIVE
Google Workspace Enterprise Identity, access, and endpoint management	✓ ACTIVE
Subprocessor SOC 2 Compliance All third-party AI providers independently certified	✓ VERIFIED
Canadian Data Residency (Primary) Core databases and processing in Montréal, Canada	✓ ACTIVE

INFRASTRUCTURE & CLOUD ARCHITECTURE

Built on Google Cloud — Anchored in Canada

The Karmaflow.ai platform is hosted entirely on Google Cloud Platform (GCP), leveraging enterprise-tier infrastructure with multi-layer security controls. All primary application workloads, databases, and data processing pipelines are provisioned within Canadian regions (Montréal,

Québec), ensuring that member and client data remains subject to Canadian privacy law (PIPEDA) by default.

Primary Region: Google Cloud — Montréal, Canada (northamerica-northeast1)
Data Processing: All core databases, application logic, and analytics remain in Canada
LLM Processing: OpenAI and Google AI APIs (USA) — transit only, no persistent storage
Network Security: VPC isolation, private service connect, cloud armor WAF, DDoS protection

Google Cloud's infrastructure provides a defense-in-depth security model including physical data centre security (ISO 27001 certified), hardware security modules, encryption at rest and in transit, and continuous vulnerability management — all inherited by the Karmaflow.ai platform.

DATA GOVERNANCE & SOVEREIGNTY

What Stays in Canada — What Leaves and Why

Karmaflow.ai distinguishes clearly between primary data — which is always retained within Canadian infrastructure — and transient processing data passed to AI model APIs for inference only.

STAYS IN CANADA	USA — TRANSIENT ONLY
· Member & client PII · Conversation logs & analytics · Business intelligence data · Application databases · Audit logs & access records	· LLM inference via OpenAI API (no storage) · LLM inference via Google AI API (no storage) · Voice synthesis via Cartesia (transient) · Speech recognition via Deepgram (transient) · **No subprocessor retains or trains on data**

THIRD-PARTY SUBPROCESSORS

Vetted, SOC 2-Compliant AI Infrastructure Partners

Karmaflow.ai engages a limited number of specialized AI infrastructure providers as subprocessors. Each has been independently assessed for SOC 2 compliance. Contractually, none are permitted to store, retain, or use client data for model training or any secondary purpose.

Subprocessor	Role	Data Location	SOC 2 Status
OpenAI	Large language model inference (GPT-4 series)	USA	SOC 2 Type II
Google AI (Gemini)	Large language model inference (Gemini series)	USA	ISO 27001 / Enterprise
Deepgram	Real-time speech-to-text recognition	USA	SOC 2 Type II
Cartesia	Neural text-to-speech voice synthesis	USA	SOC 2 Type II
LiveKit	Real-time WebRTC voice infrastructure	USA	SOC 2 Type II
Twilio	SMS & voice communications delivery	USA	SOC 2 Type II
Mailgun	Transactional email delivery	USA	SOC 2 Type II

All subprocessor engagements are governed by Data Processing Agreements (DPAs) that explicitly prohibit secondary use, training, or retention of client data. API communications are encrypted in transit using TLS 1.3.

Subprocessor Log Retention & Customer Rights

Each subprocessor temporarily retains operational logs for a defined period in accordance with their individual data retention policies. These logs may include transactional metadata, delivery records, or session diagnostics generated during service operation. Karmaflow.ai clients are entitled to request access to, or a copy of, any logs pertaining to their account at any time.

Select subprocessors also support negotiated reductions to their default log retention windows. Clients with heightened compliance requirements — such as sector-specific privacy mandates or internal data minimization policies — may formally request a shortened retention period. Karmaflow.ai will facilitate these requests on the client's behalf as part of its enterprise compliance support obligations.

IDENTITY, ACCESS & INTERNAL CONTROLS

Zero Trust Posture — Google Workspace Enterprise

Karmaflow.ai operates a Zero Trust security model for all internal access. Identity is the new perimeter. Every access decision — to infrastructure, data, or systems — is authenticated, authorized, and logged.

1 Google Workspace Enterprise Identity Management

- SSO enforced across all internal systems and cloud services
- Phishing-resistant MFA (FIDO2/hardware keys) required for all staff
- Context-aware access policies — device trust, IP, and risk signals evaluated per request
- Privileged access reviewed quarterly; least-privilege principle enforced

2 Google Cloud Infrastructure Security

- VPC Service Controls isolate sensitive data perimeters
- IAM roles strictly scoped by function — no shared credentials, no standing admin access
- Cloud Armor WAF and DDoS mitigation on all public-facing endpoints
- Binary Authorization and container signing for all deployed workloads
- Security Command Center continuously monitors for misconfigurations and threats

3 Proxy-Aware & Contextual Access Controls

- All outbound API calls route through controlled egress with logging
- Contextual access evaluates user identity, device health, location, and time of access
- Access to production environments requires just-in-time (JIT) approval
- All administrative actions are logged to an immutable audit trail

4 Encryption & Data Protection

- Data at rest: AES-256 encryption managed via Google Cloud KMS
- Data in transit: TLS 1.3 enforced on all internal and external communications
- Secrets management: Google Secret Manager — no secrets in code or environment variables
- Database access: encrypted connections only, no direct public exposure

ORGANIZATIONAL SECURITY PRACTICES

People, Process & Policy

Security at Karmaflow.ai is an organizational discipline, not just a technical one. Our internal practices are designed to eliminate the most common vectors for enterprise data breaches.

- **No outsourced or offshore personnel.** All Karmaflow.ai team members are located in Canada. We do not engage offshore contractors or outsourced development resources for any work involving client data or production systems.

- **Background screening.** All employees and contractors with system access undergo background checks prior to onboarding.

- **Security awareness training.** All staff complete mandatory security awareness training at onboarding and annually thereafter, covering phishing, social engineering, and data handling protocols.

- **Incident response plan.** A documented Incident Response Plan (IRP) is maintained and tested annually. Client notification procedures comply with PIPEDA breach reporting requirements.

- **Vulnerability management.** Dependencies are continuously scanned using automated tooling. Critical patches are applied within defined SLA windows; infrastructure is regularly assessed.

- **Vendor risk management.** All third-party vendors with data access are assessed for security posture and subject to contractual data protection obligations before engagement.

- **Change management.** All infrastructure and code changes follow a peer-reviewed, CI/CD pipeline with automated security scanning. No direct production changes are permitted outside the change control process.

Questions or Requests for Additional Detail?

Enterprise clients and partners may request our full security documentation package, subprocessor DPAs, or a security review session with our team.

security@karmaflow.ai