Client Culture — Platform Security Overview

Version 2026-04-15

1. Introduction

Client Culture handles sensitive client feedback and business data on behalf of professional services firms. This document describes our security practices — the infrastructure we run on, the controls we apply, and the choices we've made to minimise exposure.

It supersedes all prior versions. If you have questions about anything in this document, contact security@clientculture.com.

2. Company & Regulatory Posture

Client Culture Pty Ltd is incorporated in Australia. We operate under:

- The Australian Privacy Act 1988 and the Australian Privacy Principles (APPs)
- The UK GDPR for data relating to UK residents
- The EU GDPR for data relating to EEA residents

When we handle survey responses on behalf of a firm, we act as a data processor under GDPR Article 28. The firm is the data controller and gives us instructions on what data to collect and how to process it. All processing is governed by a written data processing agreement between Client Culture and each firm.

3. Data We Handle

We collect only the data our clients direct us to collect. This typically includes:

- Client contact records — names, emails, and firm relationships, provided by the firm
- Survey responses — NPS scores, loyalty driver selections, and verbatim comments
- Staff records — names, emails, roles, team and office assignments

- Authentication data — account email, SSO identifiers, and session state

All data collected remains the property of the firm, not Client Culture. We do not sell personal data, and we do not use it for advertising or cross-firm analytics.

4. Infrastructure

Client Culture runs on a consolidated, single-cloud platform hosted on Amazon Web Services infrastructure via managed providers:

Component	Provider	Region
Application & edge compute	Vercel	Singapore (ap-southeast-1)
Database	Prisma Postgres	Singapore (ap-southeast-1)
Transactional and survey email	Resend	Tokyo (ap-northeast-1)
AI analysis (anonymised data only)	OpenAI (see EphemeralAI for details)	US

Vercel, Prisma Postgres, and Resend all operate on AWS infrastructure. Every sub-processor that handles personally-identifiable customer data is hosted in Asia-Pacific (Singapore or Tokyo). The only US-located sub-processor is OpenAI, which receives fully anonymised text — no respondent names, emails, or identifying details ever leave the Asia-Pacific region in identifiable form.

The platform is built on Next.js 15 (App Router). Code changes are committed to a GitHub repository, which is connected to Vercel's Git-integrated CI/CD system. Vercel automatically builds and deploys each commit — production releases come from the `main` branch, and isolated preview deployments are available for any branch or pull request when needed.

5. Encryption

In transit. TLS 1.2+ is enforced on all connections between clients and the platform, and between the platform and all outbound services (including email delivery). Vercel's edge negotiates the strongest cipher supported by each client.

At rest. The primary database uses AES-256 encryption at rest, managed by Prisma Postgres on AWS infrastructure. Encryption keys are held in HSM-backed key management services at the infrastructure provider level.

Application-layer encryption. Per-firm SSO client secrets are encrypted at rest with AES-256-GCM using a platform-managed key before they reach the database, providing an additional layer of protection for tenant-specific credentials.

6. Authentication & Access Control

User authentication is handled via passwordless sign-in:

- Enterprise Single Sign-On via Microsoft Entra ID, configured per firm with the firm's own tenant. Tenant validation is enforced at login — users from unapproved tenants cannot authenticate even if they know the client ID.
- Passwordless authentication via Microsoft for firms that haven't configured their own SSO.

We do not store user passwords. No password-based authentication is available to end users.

Role-based access control is applied throughout the platform:

- Role hierarchies are configured per firm (admin, managing partner, division head, office head, team leader, individual contributor)
- Data visibility is scoped to the user's role — individuals see their own client portfolio, team leaders see their team, office heads see their office, and so on
- Firm-wide access is reserved for administrators and managing partners
- Every visibility query flows through a central visibility engine that enforces these rules consistently

Audit logging captures all administrative actions, including user impersonation by support staff. Impersonation is restricted to platform super-admins (Client Culture internal staff) and firm admins (within their own firm boundary). All impersonation events are time-limited, session-bound, and logged.

7. Application Security

The platform is built on Next.js 15 with React Server Components, which provide framework-level protections against common web vulnerabilities.

- No raw SQL. All database access flows through the Prisma ORM with parameterised queries. The only raw SQL usage in the codebase is for read-only health checks.
- Input validation. Sensitive API routes (authentication, survey submission, campaign operations, report generation) use Zod schemas to validate all incoming data before it reaches business logic.
- Type-safe database access. TypeScript and Prisma enforce schema correctness at compile time across all data operations.
- CSRF protection. Authenticated endpoints are guarded by a CSRF token mechanism with `__Host-` prefixed cookies.
- XSS protection. React's automatic output escaping prevents injection of untrusted content into the DOM.
- Rate limiting. Public endpoints (survey submission, unsubscribe), authentication routes, and expensive AI operations enforce per-IP rate limits to prevent abuse.
- Bot and spam protection. Survey submissions are protected by a honeypot field and a minimum-time-on-page gate that filters automated traffic. Kudos submissions additionally run through content quality checks to filter spam and low-quality text.

8. Email Security

All outbound email is delivered through Resend with full authentication:

- Dedicated sending subdomain. `send.clientculture.com` is delegated to Resend for envelope sender and bounce path, keeping mail flows isolated from the rest of the domain.
- SPF and DKIM. The sending domain is fully authenticated. DKIM signing is aligned with `clientculture.com` for DMARC compliance.

- Reply-To routing. Survey emails set `Reply-To` to the relevant firm professional, so responses reach the right person without leaking the platform's internal addresses.
- One-click unsubscribe. Every survey email includes a `List-Unsubscribe` header (RFC 8058) and a visible unsubscribe link. Unsubscribes are honoured permanently and applied across all future campaigns from the firm.

9. Ephemeral Data Retention

Client feedback is sensitive. Our Ephemeral Data Retention framework gives each firm direct control over how long verbatim comments are retained — from same-day deletion for firms with strict data minimisation requirements, through to extended retention for firms that want longer review windows. No other client feedback platform offers this level of firm-controlled retention.

Structured data persists. NPS scores, loyalty driver selections, and response metadata (dates sent and submitted, and the assigned professional) are retained indefinitely as structured data. This is what powers trend charts, benchmarks, and longitudinal reports — none of it contains free-text content or personal identifiers beyond the relationship pairing required for reporting.

Verbatim comments expire on your schedule. The free-text comments in a survey response are retained only for the period each firm chooses. A scheduled cleanup job runs hourly to enforce each firm's retention setting. Expired survey invitations are automatically anonymised. No manual intervention is required.

Same-day deletion is available for firms with the strictest data minimisation policies.

10. EphemeralAI™ Processing

When AI is used in our platform, we apply controls matched to the product and the data involved. Most of our platform uses no third-party AI at all — dashboards, trend charts, NPS benchmarks, and longitudinal reports all run on structured data we hold ourselves. We use AI in three specific features:

Custom Reports — available to all firms.
AI assists with drafting executive commentary in client experience reports. Aggregate scores, driver selections, and verbatim feedback are sent to OpenAI under their enterprise data processing agreement. OpenAI is contractually prohibited from training their models on this submitted data, all transmission is encrypted, and the OpenAI API is SOC 2 compliant. Every report is reviewed and customised by our team before delivery to the firm.

Advisory Preparation Assistant — available for firm pilots.
Helps professionals draft client advice and memos from their firm's knowledge base. Personal identifiers (names, email addresses, organisation names, phone numbers) are detected and stripped by an anonymisation service before any data reaches OpenAI. The AI receives only anonymised, de-identified text — OpenAI never sees respondents' names, email addresses, or other identifying details.

Horizon Scanning Tool — available for firm pilots.
A proactive advisory tool that surfaces relevant legislative, regulatory, and market developments for professionals' clients. Same anonymisation posture as the Advisory Preparation Assistant — full PII stripping before any AI call.

AI is not used for routine dashboard analytics, theme extraction across all feedback, or any background processing. It runs only when a user explicitly triggers one of these three features.

11. Data Retention & Deletion

Survey data is retained for up to four years by default, and each firm can configure shorter retention:

- Verbatim comments: configurable from 0 days (same-day deletion) upward, per firm
- Personal identifiers on expired survey invitations: automatically anonymised when the invitation expires
- Structured aggregate data: retained for longitudinal reporting

Deletion requests. Individuals can request deletion of their data by contacting their firm (the data controller). We action deletion requests within two weeks. Archived and backup copies are destroyed within 90 days thereafter.

Firm offboarding. If a firm ceases to use the platform, their data is deleted from production systems within 30 days of account closure and from backups within 90 days.

12. Sub-Processors

We use a small number of trusted third-party services to operate the platform. All sub-processors are contractually bound under data processing agreements that meet GDPR Article 28 and APP 8 requirements.

Component	Provider	Region
Application & edge compute	Vercel	Singapore (ap-southeast-1)
Database	Prisma Postgres	Singapore (ap-southeast-1)
Transactional and survey email	Resend	Tokyo (ap-northeast-1)
AI analysis (anonymised data only)	OpenAI (see EphemeralAI for details)	US

Vercel, Prisma Postgres, and Resend all operate on Amazon Web Services infrastructure. Details of downstream sub-processors are available in each provider's own trust documentation. We will notify customers of any material changes to our sub-processor list.

13. Backups & Business Continuity

Automated backups. The production database is backed up daily with a 30-day point-in-time restore window, provided by Prisma Postgres on the Business plan.

Availability. The application runs on Vercel's global edge network with automatic failover and health monitoring. A continuous health-check probes the database every 5 minutes and alerts on degradation.

Disaster recovery. In the event of a regional outage affecting our primary Singapore region, the application's stateless compute layer can be redirected to other Vercel regions while database recovery proceeds from the most recent backup.

14. Incident Response

Client Culture maintains an incident response policy covering:

- Initial detection and triage
- Investigation and containment
- Customer notification, where affected firms and individuals are identified
- Root-cause analysis and remediation
- Post-incident review and preventive changes

Should a security incident affect our customers, we will notify affected firms promptly and work with them to meet any statutory breach notification obligations under the Australian Privacy Act, UK GDPR, or EU GDPR.

15. Secure Development

- All code changes flow through version control (GitHub) and Vercel's automated build and deploy pipeline. Production releases are deployed from the `main` branch; preview deployments are available on demand for branch-based testing
- Production access is restricted to a small number of senior engineers
- Dependency vulnerabilities are monitored via automated scanning. High-severity vulnerabilities are addressed on a defined schedule
- All employees sign non-disclosure agreements on hire, and ongoing access to customer data is limited to roles that genuinely require it

16. Contact

For security questions, vulnerability reports, or to request additional documentation:

- security@clientculture.com — security and vulnerability matters
- privacy@clientculture.com — data protection and privacy matters

This document is reviewed and updated as the platform evolves. The date at the top of this document indicates the most recent revision.

Client Culture Pty Ltd · Australia · clientculture.com