

# VENDOR SECURITY QUESTIONNAIRE

Pre-filled responses for enterprise IT, security, and procurement teams

Covers: SIG Lite, CAIQ, and standard enterprise due diligence questionnaires

Version 1.0 — April 2026 — Contact [legal@teamcalendar.ai](mailto:legal@teamcalendar.ai) for additional questions

Company	HQ	Infrastructure	Security contact
Calndr Inc.	Mountain View, CA, USA	AWS (US-East, US-West)	<a href="mailto:security@teamcalendar.ai">security@teamcalendar.ai</a>

## A. COMPANY & GOVERNANCE

#	Question	TEAMCAL AI Response
A1	What type of company is TEAMCAL AI?	Calndr Inc. is a privately held corporation incorporated in California, USA. We provide AI-powered team scheduling software (SaaS) under the brand TEAMCAL AI, including the Zara AI scheduling assistant. <i>Principal office: 855 Maude Ave, Mountain View, CA 94043</i>
A2	How long has the company been in operation?	TEAMCAL AI has been operating since 2019. The platform is in active production, serving customers across 90+ countries.
A3	Does TEAMCAL AI have a dedicated security function?	Yes. Security responsibilities are managed by the founding team with defined ownership of vulnerability management, incident response, and compliance. Security contact: <a href="mailto:security@teamcalendar.ai">security@teamcalendar.ai</a>
A4	Does TEAMCAL AI have a written information security policy?	Yes. TEAMCAL AI maintains written information security policies covering access control, data classification, incident response, change management, and employee security. These are available upon request under NDA.
A5	Does TEAMCAL AI conduct background checks on employees?	Yes. All employees undergo pre-employment background checks as a condition of employment, in addition to security and privacy training at onboarding.
A6	Does TEAMCAL AI have cyber liability insurance?	Yes. TEAMCAL AI maintains cyber liability insurance. Certificate of Insurance available upon request.
A7	Does TEAMCAL AI have a Business Continuity / Disaster Recovery plan?	Yes. TEAMCAL AI maintains a documented DR plan with RTO of 4 hours and RPO of 24 hours. Backups are stored in AWS S3 with 30-day retention.

## B. DATA HANDLING & PRIVACY

#	Question	TEAMCAL AI Response
B1	What customer data does TEAMCAL AI collect and	TEAMCAL AI stores: account data (name, email, title),

#	Question	TEAMCAL AI Response
	store?	OAuth tokens (encrypted), meeting scheduling metadata (time, duration, attendee emails for scheduled meetings), usage logs, and billing status. Payment card details are handled by Stripe and never reach TEAMCAL AI servers.
B2	Does TEAMCAL AI store calendar event content?	NO. This is an architectural guarantee, not a policy. Calendar events, meeting titles, attendee names within calendar events, notes, and attachments are never written to TEAMCAL AI databases. Calendar data is queried in real time via OAuth solely to determine free/busy windows and is discarded immediately after use. <i>This eliminates calendar data exposure at rest entirely.</i>
B3	Where is customer data stored geographically?	All data is stored in AWS US-East and US-West regions. Customers requiring EU data residency should contact <a href="mailto:legal@teamcalendar.ai">legal@teamcalendar.ai</a> to discuss available options.
B4	Does TEAMCAL AI sell customer data to third parties?	No. TEAMCAL AI does not sell, rent, or trade customer data. Data is used exclusively to provide the Services described in the MSA.
B5	Does TEAMCAL AI use customer data to train AI models?	No. Customer data is not used for AI model training. TEAMCAL AI's LLM and AI usage policy is documented at <a href="https://teamcal.ai/llm">teamcal.ai/llm</a> .
B6	Is TEAMCAL AI GDPR compliant?	Yes. TEAMCAL AI maintains a GDPR compliance programme covering lawful basis, data subject rights, DPA, SCCs for international transfers, and privacy notices. A signed DPA and EU SCC Addendum (Module 2) are available for EU-based customers.
B7	Is TEAMCAL AI CCPA compliant?	Yes. TEAMCAL AI supports California resident rights including access, deletion, and opt-out of sale (TEAMCAL AI does not sell data). Privacy disclosures are at <a href="https://teamcal.ai/privacy">teamcal.ai/privacy</a> .
B8	What is the data retention period?	Account and scheduling data: retained for the subscription duration plus 30 days. Usage logs: 90 days. Billing records: 7 years (legal obligation). Full policy at <a href="https://teamcal.ai">teamcal.ai</a> and available as a downloadable document.
B9	How is data deleted upon contract termination?	All customer data is deleted within 30 days of contract termination. Customers may request a data export before deletion. Written deletion certification is provided within 35 days.
B10	Does TEAMCAL AI have a documented Data Processing Agreement (DPA)?	Yes. A signed DPA is provided to all ClientSync and Enterprise customers and is available for download at <a href="https://trust.teamcal.ai">trust.teamcal.ai</a> .

## C. SECURITY CONTROLS

#	Question	TEAMCAL AI Response
C1	How is data encrypted in transit?	All data in transit is encrypted using TLS 1.2 or higher with SHA-256 and RSA encryption. This applies to all browser-to-server, API, and integration communications.
C2	How is data encrypted at rest?	All data at rest is encrypted using AES-256 on AWS infrastructure. This includes databases, backups, read replicas, and snapshots.
C3	How are passwords stored?	User passwords are stored as salted cryptographic hashes. Plaintext passwords are never stored or transmitted. TEAMCAL AI also supports OAuth 2.0 (Google, Microsoft) as the preferred authentication method.
C4	Does TEAMCAL AI support Single Sign-On (SSO)?	Yes. TEAMCAL AI supports SSO via Google Workspace and Microsoft 365, inheriting the organisation's existing MFA and authentication policies.
C5	Does TEAMCAL AI support multi-factor authentication (MFA)?	Yes. 2FA/MFA is available for all user accounts. ClientSync and Enterprise plan administrators can enforce org-wide MFA requiring all users to complete 2FA setup at next login.
C6	Does TEAMCAL AI support SAML-based SSO or SCIM provisioning?	SAML SSO: currently via Google and Microsoft OAuth. Dedicated SAML SSO (Okta, Azure AD) is on the roadmap. SCIM directory provisioning is on the roadmap for Enterprise. Contact <a href="mailto:legal@teamcalendar.ai">legal@teamcalendar.ai</a> to discuss current enterprise options. <i>Timeline available upon request.</i>
C7	Does TEAMCAL AI have role-based access control (RBAC)?	Yes. Within organisations, account administrators control user permissions, team memberships, and integration access. Admin-level controls are available to IT administrators through the admin panel.
C8	How does TEAMCAL AI handle third-party calendar credentials?	TEAMCAL AI uses OAuth 2.0 for all calendar integrations. TEAMCAL AI never stores or sees calendar passwords. OAuth tokens are encrypted at rest and users can revoke access at any time from their account settings.
C9	Does TEAMCAL AI conduct vulnerability scanning?	Yes. TEAMCAL AI conducts automated vulnerability scanning of code repositories for vulnerable dependencies. AWS infrastructure is continuously scanned by AWS native security tools. Host-based firewalls are maintained on all services.
C10	Does TEAMCAL AI conduct penetration testing?	TEAMCAL AI conducts periodic security reviews. We are moving toward annual formal penetration tests by a qualified third-party firm. Results are available to Enterprise customers under NDA.

#	Question	TEAMCAL AI Response
C11	How are security patches applied?	Security patches are applied as part of TEAMCAL AI's continuous integration pipeline. Critical vulnerabilities (CVSS 9+) are patched within 24 hours of availability. Services run in containers enabling rapid redeployment.
C12	Does TEAMCAL AI log and monitor access?	Yes. TEAMCAL AI maintains audit logs for login events, data access, and administrative actions. Logs are retained for 90 days in production systems and archived for security incidents.

## D. INFRASTRUCTURE & AVAILABILITY

#	Question	TEAMCAL AI Response
D1	Where is the TEAMCAL AI platform hosted?	TEAMCAL AI is hosted on Amazon Web Services (AWS) in the US-East and US-West regions. AWS maintains 98+ security standards and compliance certifications including ISO 27001, SOC 1/2/3, PCI DSS, and FedRAMP.
D2	Does TEAMCAL AI have a documented uptime SLA?	Yes. ClientSync and Enterprise plans carry a 99.9% monthly uptime commitment with a defined service credit schedule. The full SLA document is available at <a href="https://trust.teamcal.ai">trust.teamcal.ai</a> .
D3	Does TEAMCAL AI have a public status page?	A status page is being implemented at <a href="https://status.teamcal.ai">status.teamcal.ai</a> . Current status and incident notifications are communicated to customers via email. Customers may subscribe to incident alerts.
D4	How does TEAMCAL AI handle disaster recovery?	Recovery Time Objective (RTO): 4 hours. Recovery Point Objective (RPO): 24 hours. Daily backups are stored in AWS S3 with 30-day retention. Secondary backups are maintained in a separate AWS region.
D5	Are services containerised and isolated?	Yes. All TEAMCAL AI services run in containers (LXC) that isolate processes, memory, and the file system. This limits blast radius for any potential incident and enables rapid redeployment.
D6	Does TEAMCAL AI use a CDN?	Static assets are served via CDN. Application data flows directly through the AWS-hosted application layer, not via third-party CDN providers.
D7	What is the change management process?	All code changes require unit, integration, and end-to-end tests, peer code review, QA review, and post-deployment monitoring. Changes are tracked through version control with full audit trail.

## E. COMPLIANCE & CERTIFICATIONS

#	Question	TEAMCAL AI Response
E1	Is TEAMCAL AI SOC 2 certified?	TEAMCAL AI is currently in SOC 2 Type II readiness. We anticipate completing the audit in 2026. AWS infrastructure (our hosting provider) holds SOC 1, SOC 2, and SOC 3 certifications. Security controls documentation is available at <a href="https://trust.teamcal.ai">trust.teamcal.ai</a> .
E2	Is TEAMCAL AI ISO 27001 certified?	Not currently. TEAMCAL AI's security controls align with ISO 27001 principles and AWS infrastructure is ISO 27001 certified. ISO 27001 certification is on our compliance roadmap.
E3	Is TEAMCAL AI PCI DSS compliant?	TEAMCAL AI uses Stripe for all payment processing. Stripe is PCI DSS Level 1 certified. TEAMCAL AI's servers never receive or store payment card data — all payment data flows directly to Stripe via their JavaScript integration.
E4	Is TEAMCAL AI GDPR compliant?	Yes. TEAMCAL AI maintains an active GDPR compliance programme. Signed DPA and EU SCC Addendum (Module 2) are available. Full documentation at <a href="https://trust.teamcal.ai">trust.teamcal.ai</a> .
E5	Is TEAMCAL AI HIPAA compliant?	TEAMCAL AI will execute a Business Associate Agreement (BAA) with healthcare customers. TEAMCAL AI does not store calendar event content (which may contain PHI). BAA available upon request.
E6	Does TEAMCAL AI have a formal incident response plan?	Yes. TEAMCAL AI maintains a documented incident response plan covering identification, containment, recovery, and post-incident review. Breach notifications are provided within 72 hours of confirmation per GDPR and within 60 days per HIPAA BAA.
E7	Does TEAMCAL AI respond to security questionnaires?	Yes. This document is TEAMCAL AI's standard security questionnaire response. For additional questions or an onsite security review for Enterprise contracts, contact <a href="mailto:legal@teamcalendar.ai">legal@teamcalendar.ai</a> . <i>Additional detail available under NDA.</i>

## F. THIRD-PARTY & SUPPLY CHAIN

#	Question	TEAMCAL AI Response
F1	What third-party sub-processors does TEAMCAL AI use?	Amazon Web Services (cloud infrastructure, US regions); Stripe Inc. (payment processing only — no scheduling data shared). A full sub-processor list is available in the TEAMCAL AI DPA.
F2	How does TEAMCAL AI vet sub-processors?	All sub-processors are required to maintain security standards equivalent to TEAMCAL AI's own, including data processing agreements. Sub-processors are reviewed annually.

#	Question	TEAMCAL AI Response
F3	Does TEAMCAL AI use open-source software?	Yes. TEAMCAL AI uses open-source components. All dependencies are tracked in version control and scanned for vulnerabilities automatically. Critical CVEs are patched within 24 hours.
F4	Does TEAMCAL AI conduct supply chain risk assessments?	Yes. TEAMCAL AI's engineering process includes automated scanning of all third-party dependencies via continuous integration tooling.

## G. ACCESS MANAGEMENT

#	Question	TEAMCAL AI Response
G1	How does TEAMCAL AI manage internal access to customer data?	Access to customer data is granted on a strict need-to-know basis. All internal access is logged. Access rights are reviewed quarterly and revoked immediately upon role change or departure.
G2	Does TEAMCAL AI have a privileged access management (PAM) programme?	Yes. Privileged access to production systems requires multi-factor authentication and is logged with full audit trails. Access credentials are managed via secure credential management practices.
G3	How are terminated employees' access rights handled?	Access to all systems is revoked immediately upon employment termination. This is a mandatory step in the offboarding checklist executed by the operations team.
G4	Can customers revoke TEAMCAL AI's access to their calendar systems?	Yes. Users can disconnect any calendar integration (Google, Outlook) at any time from their account settings. OAuth tokens are immediately revoked and deleted upon disconnection.

### Additional questions or need a custom security review?

Contact: [legal@teamcalendar.ai](mailto:legal@teamcalendar.ai) • Security: [security@teamcalendar.ai](mailto:security@teamcalendar.ai)

Trust center: [trust.teamcal.ai](https://trust.teamcal.ai) • Additional documentation available under NDA for Enterprise accounts

*All responses in this document are accurate as of April 2026 and subject to change. TEAMCAL AI will notify customers of material changes to its security programme.*