Information Security Policy

Creative Media Innovation (PTY) LTD | CMI Bridge SaaS Platform

Effective Date: 14 July 2026 | Version: 2.0

This Information Security Policy ('Policy') describes the security practices and controls that Creative Media Innovation (PTY) LTD ('Company') applies to protect the confidentiality, integrity, and availability of the Platform and Customer Data. It is published to give Customers transparency into how the Platform is actually built and operated. It is provided for informational purposes and does not form part of any agreement unless expressly incorporated in writing.

Commitment: The Company maintains a security programme proportionate to its size and the sensitivity of the data it processes, built on managed cloud infrastructure with strong security defaults, and strengthened continuously as the Company grows (see Section 13, Security Roadmap).

1. Scope

This Policy applies to all systems, infrastructure, personnel, and processes involved in the delivery and operation of the Platform, including cloud infrastructure, application code, data storage, and third-party services. It covers Customer Data processed through the Platform and the Company's internal information assets.

2. Governance and Responsibility

2.1 Security Ownership

The Company's designated Information Officer (who also oversees POPIA compliance) is responsible for information security, including:

- Maintaining and reviewing this Policy at least annually;
- Overseeing the security posture of the Platform and its third-party providers;
- Coordinating the response to security incidents and vulnerability reports;
- Ensuring security is considered in the design of new features before release.

2.2 Personnel

The Company operates with a small, focused team. All personnel with access to production systems or Customer Data:

- Are bound by confidentiality obligations;
- Access Customer Data only as necessary to operate and support the Platform;
- Report any suspected security incident to the Information Officer immediately.

3. Data Classification and Handling

The Company classifies information into the following categories and applies controls accordingly:

Classification	Examples	Controls

Confidential	Customer Data, personal data, credentials, source code, financial records	Encryption at rest and in transit, strict access controls, audit logging
Internal	Internal communications, operational procedures, employee data	Role-based access, need-to-know basis, standard access controls
Public	Marketing materials, public documentation, this Policy	No special restrictions

4. Hosting and Infrastructure

The Platform is built entirely on Google Firebase and Google Cloud Platform. The Company does not operate its own servers or data centres, and Customer Data is hosted exclusively in Google Cloud:

- Physical security, hardware lifecycle, and network infrastructure are managed by Google, whose data centres maintain independent certifications including ISO/IEC 27001 and SOC 1/2/3 (see cloud.google.com/security/compliance);
- Customer Data is stored in Cloud Firestore and Cloud Storage with automatic replication across multiple regions for durability and availability;
- Access to production infrastructure is restricted to named accounts held by designated personnel; shared or generic accounts are not used;
- Application secrets (API keys and service credentials) are managed in Google Secret Manager and injected at deploy time, separate from application source code.

5. Encryption

- **In transit:** all data transmitted between users and the Platform is encrypted using TLS 1.2 or higher;
- **At rest:** all Customer Data is encrypted at rest (AES-256) by Google Cloud's default encryption;
- **Key management:** encryption keys are managed by Google Cloud's key management infrastructure as part of the managed platform;
- **Payment data:** card details are never transmitted to or stored on Company systems. All payments are processed by Stripe and Paystack, both certified to PCI DSS Level 1.

6. Access Control

6.1 Tenant Isolation

The Platform is multi-tenant. Isolation between tenants is enforced server-side by Firebase Security Rules: every read and write is evaluated against the requesting user's authenticated identity, tenant membership, active status, and role before any data is returned or modified.

6.2 Role-Based Access Control

Access within a tenant follows least privilege through five defined roles (Administrator, Manager, Operator, Clerk, and Supplier), each mapped to a granular set of more than 60 discrete

permissions. Supplier accounts are limited to a read-only portal showing only that supplier's own records.

6.3 Authentication

- User authentication is provided by Firebase Authentication (Google). Passwords are hashed and stored by Google and are never visible to the Company;
- Sessions use short-lived tokens that are refreshed automatically; when an account is deactivated, access is revoked both in the security rules and by forced sign-out;
- Administrative access to production infrastructure is via named Google accounts restricted to designated personnel;
- Multi-factor authentication for Platform user accounts is not yet available in-app; it is a committed roadmap item (Section 13).

7. Application Safeguards

- **Abuse protection:** the Platform uses Firebase App Check with reCAPTCHA v3 to identify traffic originating from unauthorised clients;
- **Live streaming:** remote machine-monitoring streams are protected by short-lived, server-issued access tokens scoped to a specific streaming session. Streams are live-only and are not recorded or stored;
- **Error monitoring:** application errors and performance are monitored through Sentry, with diagnostic data minimised and retained for approximately 90 days.

8. Development and Change Management

- All application source code is maintained under version control with full change history;
- Changes are released as versioned builds with a maintained changelog;
- Changes are tested before being deployed to production;
- Production configuration and credentials are injected at build or deploy time and are not stored in application source code;
- Third-party dependencies are reviewed and updated on a regular basis, and published security advisories for the technology stack are monitored.

9. Monitoring and Logging

- Application errors, crashes, and performance regressions are reported continuously to Sentry and reviewed by the Information Officer;
- Infrastructure, function execution, and access logs are captured by Google Cloud Logging and retained in accordance with Google Cloud's retention periods;
- Anomalies and suspected incidents are investigated under Section 12.

10. Availability and Resilience

- The Platform runs on serverless, auto-scaling Google infrastructure spanning multiple availability zones;
- Customer Data in Cloud Firestore is replicated automatically across multiple regions;
- Platform availability is underpinned by Google Cloud's published service level agreements;

- Scheduled backups with point-in-time recovery are a roadmap item (Section 13).

11. Third Parties and Subprocessors

The Company maintains a register of the third-party providers that process Customer Data (published as the Subprocessors List). Before engaging a provider, the Company reviews its published security documentation and independent certifications (for example SOC 2 or ISO/IEC 27001). Each provider is bound by data-protection terms as described in the Data Processing Agreement, and Customers receive at least 14 days' notice of subprocessor changes.

12. Security Incident Management

12.1 Incident Response

Upon detecting or being notified of a potential security incident, the Company will:

- Contain and assess the incident as quickly as possible;
- Notify affected Customers without undue delay, and within 72 hours where personal data is involved, consistent with the Data Processing Agreement;
- Notify the Information Regulator where required by section 22 of POPIA;
- Conduct a root cause analysis, implement corrective actions, and document the incident and remediation steps.

12.2 Responsible Disclosure

Customers, researchers, and other third parties who discover a potential security vulnerability in the Platform are encouraged to report it responsibly to:
Email: info@cmibridge.com
Subject line: Responsible Disclosure — Security Vulnerability
The Company will acknowledge reports within 2 business days and will work with reporters in good faith to validate and address confirmed vulnerabilities.

13. Security Roadmap

The Company is transparent about controls that are planned but not yet in place. Current roadmap items include:

- Multi-factor authentication (MFA) for Platform user accounts;
- Scheduled database backups with point-in-time recovery;
- Moving abuse protection (App Check) from monitoring to enforcement mode;
- An independent external security assessment of the Platform;
- In-app consent management for diagnostics and analytics;
- Formal certification frameworks (such as SOC 2 or ISO/IEC 27001) as customer and market requirements dictate.

Roadmap items are statements of intent, not contractual commitments, and their sequencing may change.

14. Compliance

The Company processes personal information in accordance with the Protection of Personal Information Act 4 of 2013 (POPIA) and, where applicable, the EU General Data Protection Regulation (GDPR). Details of the Company's data protection practices are set out in its Privacy Policy, Data Processing Agreement, and POPIA Compliance Framework.

15. Policy Review

This Policy is reviewed at least annually by the Information Officer, or earlier following any significant change to the Platform, its infrastructure, or applicable regulatory requirements. Material updates are communicated to Customers, and version history is maintained.

16. Contact

For security-related queries, or to request further information about the Company's security practices, please contact:
Creative Media Innovation (PTY) LTD
Attn: Information Officer (Security)
Email: info@cmibridge.com
Address: 19 Nolene Street, Constantia Kloof, Johannesburg, 1709, South Africa
This Policy reflects the Company's current security practices and is subject to change as those practices evolve. Document Owner: Information Officer | Review Cycle: Annual | Next Review: July 2027