Security overview

How Storiara protects customer data, and the options available in a dedicated customer environment.

Document owner Nick Harty, Chief Technology Officer and Security Lead

Scope Shared product and dedicated customer environments **Contact** security@storiara.com

Storiara is a film production planning application. It is offered as a shared product at app.storiara.com and as a dedicated customer environment: a single-tenant environment for one customer in its own Google Cloud project. Security questions and reports go to **security@storiara.com**.

At a glance

PROTECTION	WHERE IT APPLIES
Encryption in transit with TLS and at rest	All deployments
Access decided by security rules that check project membership and role	All deployments
Daily backups kept 7 days, with file copies held in two other regions	All deployments
Google Cloud audit logs for administrator activity, data access and sign-in	All deployments
A separate Google Cloud project, database, file bucket and user directory for the customer	Dedicated environments
Customer-managed encryption keys in Cloud KMS for the database and files	Dedicated environments
Invitation-only accounts	Dedicated environments
Two-step sign-in with an authenticator app, available to every user	Dedicated environments
Audit entries routed to a Pub/Sub topic that a customer SIEM can subscribe to	Dedicated environments
Two-step sign-in set-up required for everyone	Dedicated environments, on request
Company single sign-on over SAML or OIDC	Dedicated environments, on request
SCIM 2.0 user provisioning	Dedicated environments, on request

On request means Storiara configures the option for the environment when the customer asks for it.

Hosting and data location

- Storiara runs on Google Cloud and Firebase: App Hosting, Cloud Functions, Firestore, Cloud Storage, Identity Platform and Secret Manager.
- The database is Cloud Firestore in Google's nam5 multi-region in the United States. Uploaded files are in Cloud Storage in us-central1.
- Google operates the data centres, the network and the operating systems. Storiara runs no servers of its own.

Customer separation

Dedicated customer environment. Each customer has its own Google Cloud project, with its own database, file bucket, user directory, functions, secrets and application backend. The customer's data is stored in that project only. A build refuses to start if an environment is pointed at the shared product project.

Shared product. Every read and write from a browser is decided by security rules that check that the person is a member of the project and what their role allows. Anything the rules do not allow is refused. Server routes make the same membership check. The rules are tested automatically against an emulator each time a change is proposed.

Sign-in and access

- Shared product: email and password with email verification, Google sign-in or Apple sign-in.
- Dedicated environments: accounts exist by invitation only. New sign-ups are refused by Identity Platform itself.
- Dedicated environments: two-step sign-in with an authenticator app (TOTP) is available to every user. An environment can be configured to require everyone to set it up before using the app.
- Dedicated environments: company single sign-on over SAML or OIDC, and SCIM 2.0 user provisioning for users, so the customer's identity provider can create, update and deactivate accounts.
- Project roles: Owner, Producer, Assistant director, Cinematographer, Department head, Accountant and Crew (view).

Encryption

- In transit: HTTPS only, with TLS and HSTS.
- At rest: Google-managed encryption keys for the database and for files.
- Dedicated environments: the database and the file bucket are encrypted with customer-managed keys in the environment's own Cloud KMS.
- Server secrets are kept in Google Secret Manager.

AI and your script

- AI features use Google Gemini models on Vertex AI. Calls are made as the server's own service account, inside the deployment's own Google Cloud project.
- Google receives the script text and pages, breakdown lists, character descriptions and budget facts needed for the feature.

- Incentive tagging sends budget line descriptions to TypeSafe for classification.
- Google Cloud's terms say customer data is not used to train its models.
- Storiara does not store prompts and does not write them to server logs. Usage records hold call counts only.
- Every amount in a budget is calculated by rules. No amount comes from a model.

Backups and recovery

- The database is backed up daily and backups are kept 7 days. Delete protection is on for the database.
- All files are copied daily to a separate bucket held in two regions, us-east1 and us-east4, away from the production region. Object versioning is on and old copies are kept 7 days.
- Recovery point objective: 48 hours. Recovery time objective: 24 hours.
- The same backups run in the shared product and in every dedicated environment.

Logging and monitoring

- Google Cloud audit logs record administrator activity at all times, and data access (admin read, data read and data write) for Firestore, Cloud Storage and sign-in.
- Every audit entry is also routed to a Pub/Sub topic, so a customer's SIEM can subscribe to the entries of its dedicated environment.
- Each project has an activity log of changes and an access log of who opened, printed, exported or sent what. The Owner and Producers can read the access log and download it as CSV.
- Where SCIM is on, a provisioning log records each account created, changed or deactivated by the identity provider.
- Cloud Monitoring alerts are sent by email for function execution errors, an unusual Firestore read rate, an unusual Firestore write rate and a Pub/Sub message that has waited too long.

Application protections

- Every response carries HSTS, `X-Content-Type-Options: nosniff`, `X-Frame-Options: SAMEORIGIN` and a referrer policy.
- A content security policy enforces `frame-ancestors`, `base-uri` and `upgrade-insecure-requests`.
- Rate limits apply to the AI routes and to other server endpoints, with counters shared across server instances.
- Cloud Functions service accounts hold only the specific roles they use.

Development and release

- All code is in GitHub. Pull requests into the beta and master branches run automated checks: type check, lint, unit tests, security rules tests against an emulator, and a production build with a smoke test and a page-size budget.
- Changes go to beta first and are then merged to master.
- Deploys sign in to Google Cloud with GitHub's own identity. No deploy key is stored.
- Dependabot security alerts are on for all of Storiara's code.
- Releases are listed at storiara.com/changelog.

Deletion

- Deleting a project removes the project and everything under it: scenes, script content, budget, people, call sheet days, personal links and logs. A deletion record is kept with who, when and counts, and no project content.
- Deleting an account transfers or deletes its projects, then removes the profile and the sign-in.
- A dedicated environment is removed at the end of an engagement by deleting its Google Cloud project, which removes the database, files, users, keys and backups together.
- Backup copies age out within 7 days.

People and devices

- Nick Harty, Chief Technology Officer and Security Lead, owns security and is the only person with administrator access to production.
- All staff work on Macs with full-disk encryption (FileVault) and a screen lock. No removable media holds company or customer data.

Compliance

Storiara is working toward SOC 2 with Vanta. Fifteen security policies are approved and maintained in Vanta, which continuously monitors Storiara's cloud, GitHub, Google Workspace and Cloudflare accounts.

Subprocessors

SUBPROCESSOR	PURPOSE
Google Cloud Platform	Hosting, database, file storage, sign-in and Vertex AI models.
Google Maps and Places	Address and place lookups for locations.
Twilio	Email and texts, such as call sheets and invitations.
Mapbox	Maps and address search.
TypeSafe	Classification of budget line descriptions for production incentive tagging.
Stripe	Subscription payments in the shared product. A dedicated environment has no billing.

Contact

Security questions and reports: security@storiara.com. Support: support@storiara.com. Privacy policy: storiara.com/privacy. Terms of service: storiara.com/terms. Product documentation: storiara.com/docs/getting-started.