Security Policy

Effective day 2 February 2020

At Tutorbook we take the protection of customer data extremely seriously. This Tutorbook Security Policy describes the organizational and technical measures Tutorbook implements platform wide designed to prevent unauthorized access, use, alteration or disclosure of customer data. The Tutorbook services operate on the Google Cloud Platform ("GCP") via Google's Firebase App Infrastructure ("Firebase"); this policy describes activities of Tutorbook within its Firebase project(s) unless otherwise specified. As you continue to learn more about Tutorbook we recommend you also review our Terms of Service and Privacy Policy.

Best Practices

Incident Response Plan

- We have implemented a formal procedure for security events and have educated all our staff on our policies.
- When security events are detected they are escalated to our emergency alias, teams are paged, notified and assembled to rapidly address the event.
- After a security event is fixed we write up a post-mortem analysis.
- The analysis is reviewed in person, distributed across the company and includes action items that will make the detection and prevention of a similar event easier in the future.
- Tutorbook will promptly notify you in writing upon verification of a security breach of the Tutorbook services that affects your data. Notification will describe the breach and the status of Tutorbook's investigation.

Build Process Automation

- We have functioning, frequently used automation in place so that we can safely and reliably rollout changes to both our application and operating platform within minutes.
- We typically deploy code dozens of times a day, so we have high confidence that we can get a security fix out quickly when required.

Infrastructure

- All of our services run in the cloud. Tutorbook does not run our own routers, load balancers, DNS servers, or physical servers.

- All of our services and data are hosted in Firebase-supported GCP facilities in the USA and protected by Google security, as described at https://firebase.google.com/support/privacy.
- All of our infrastructure is spread across 3 regional GCP resource locations (one multi-region location) and will continue to work should any one of those locations fail unexpectedly. Data is stored across GCP's nam5 multi-region location that consists of the us-central1 and us-central2 regional resource locations with additional metadata stored in the Oklahoma private region. See https://cloud.google.com/security/ for details on GCP security infrastructure.
- Tutorbook uses a backup solution for datastores that contain customer data.

Data

- All customer data is stored in the USA.
- Customer data is stored in multi-tenant Firestore datastores ("Firestores"); we do not have individual datastores for each customer. However strict privacy controls exist in our application code that are designed to ensure data privacy and to prevent one customer from accessing another customer's data (i.e., logical separation). We have many unit and integration tests in place to ensure these privacy controls work as expected. These tests are run every time our codebase is updated and even one single test failing will prevent new code from being shipped to production.
- Each Tutorbook system used to process customer data is adequately configured and pathed using commercially-reasonable methods according to industry-recognized system-hardening standards.
- Tutorbook engages certain subprocessors to process customer data. These subprocessors are listed at https://tutorbook.app/legal#privacy-subprocessors as may be updated by Tutorbook from time to time.

Data Transfer

- All data sent to or from Tutorbook is encrypted in transit using 256-bit encryption.
- Our application endpoints are TLS/SSL only and score an "A+" rating on SSL Labs' tests.
- We also encrypt data at rest under an industry-standard AES-256 encryption algorithm, and each encryption key is itself encrypted with a regularly rotated set of master keys. For more information, see https://cloud.google.com/firestore/docs/server-side-encryption.

Authentication

- Tutorbook is served 100% over HTTPS.

- We have two-factor authentication (2FA) and strong password policies on GitHub, Google, and Tutorbook to ensure access to cloud services are protected.

Permissions and Admin Controls

- We implement custom Firebase Authentication claims to ensure admin and supervisor access to Tutorbook is not compromised.

Application Monitoring

- On an application level, we may produce audit logs for all activity, ship logs to our service providers for analysis, and use S3/Glacier for archival purposes.
- All access to Tutorbook applications may be logged and audited.
- All actions taken on production consoles or in the Tutorbook application may be logged.

Payment Processing

All payment instrument processing for purchase of the Tutorbook services is performed by Stripe. For more information on Stripe's security practices, please see https://stripe.com/docs/security/stripe.

Customer Responsibilities

- Managing your own user accounts and roles from within the Tutorbook services.
- Protecting your own account and user credentials by using two-factor authentication for all of your employees accessing the Tutorbook services.
- Compliance with the terms of your services agreement with Tutorbook, including with respect to compliance with laws.
- Promptly notifying Tutorbook if a user credential has been compromised or if you suspect possible suspicious activities that could negatively impact security of the Tutorbook services or your account.
- You may not perform any security penetration tests or security assessment activities without the express advance written consent of Tutorbook.

Third Parties

Security, Privacy and Compliance Information for Tutorbook

Tutorbook is a data processor and engages certain onward subprocessors that may process personal data submitted to Tutorbook's services by the controller. These subprocessors are

listed below, with a description of the service and the location where data is hosted. This list may be updated by Tutorbook from time to time:

- Alphabet, Inc. Hosting, storage, and analytics (USA)
- Intercom, Inc. In-app messaging and support (USA)
- Twilio, Inc. SMS functionality (USA)
- Stripe, Inc. Payment provider for Tutorbook customer data only (USA)