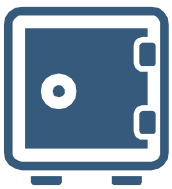
Rollbar

Security and Compliance



How Rollbar Protects Sensitive Error Data

Published: July 2017
This document is publicly available at: https://cdn.rollbar.com/assets/shared/resources/compliance.pdf
For feedback or questions, please contact: sales@rollbar.com

Introduction

At Rollbar, we believe the speed at which an organization develops software is a key determinant of its success.

The faster you develop and deliver software into the hands of users, the faster you get market feedback and realize business value.

We built Compliant SaaS to eliminate the inevitable compromise organizations make to balance speed against security and compliance.

Rollbar Compliant SaaS is designed to enable rapid software development *without* leaving gaps that may expose you to security and legal risks.

This paper outlines how we protect your data – from the technical capabilities we have built into Rollbar Compliant SaaS, such as encryption, to the physical and administrative safeguards we have instituted as part of our security program.

Our security program is led by the Chief Information Security Officer and the Chief Technology Officer of Rollbar.

Rollbar is HIPAA and ISO 27001 compliant, CSA STAR registered, and EU-US Privacy Shield certified.

Table of Contents

Compliant SaaS Product Overview

Rollbar Compliant SaaS is a cloud-based application error monitoring solution specially designed to handle sensitive data, such as PII and PHI data, in a secure and compliant manner.

Using Rollbar Compliant SaaS, organizations can avoid legal risks from mishandling sensitive data, and reduce security risks caused by bad actors.

Additionally, organizations can save time and money previously spent on de-identifying error data before sending them to cloud-based solutions, or on maintaining an on-premise error monitoring solution.

Compliant SaaS starts to collect data once the appropriate Rollbar library is integrated into an app's codebase.

It filters, groups, and visualizes the data, and send alerts – in real-time and as configured by the developer. It provides rich contextual data on each error, allowing the developer to diagnose and debug them faster.

The data is always encrypted while in transit and at rest, and is stored in SOC 2 Type 2 compliant data centers.

Visit our Rollbar Compliant SaaS page at https://rollbar.com/compliance.

Security Features

ENCRYPTION

All raw data is encrypted at rest at the application-level. Each project within a customer account is issued an encryption key, and data is decrypted only when requested by an authenticated member. This provides an additional level of protection should Rollbar ever encounter a breach.

All data in transit is sent through HTTPS (TLS) encrypted connections, ensuring confidentiality and integrity of data sent between Compliant SaaS and customer.

Rollbar Compliant SaaS uses industry-standard AES-256 GCM encryption. If the data is ever lost, it will be useless to the attacker since it would appear as randomized data.

ACCESS CONTROLS

Rollbar Compliant SaaS offers a set of enterprise access control features designed to prevent unauthorized access.

Single sign-on (SSO), based on SAML-2.0 XML standard, lets organizations control and maintain identity management for their users. Okta, Google Apps, and Bitium are supported.

Two-factor Authentication (2FA) provides an extra layer of security by requiring users to enter a time-sensitive, one-time code in addition to their own password during login.

Additionally, administrators can set policies on login attempts, password strength requirements, session expiration limits, access times, and IP whitelists.

Security Features (continued)

DATA RETENTION

Rollbar Compliant SaaS allows you to retain retrievable records, documents, and data, including PII and PHI, in their original business context.

We accommodate custom data retention policy to fit your compliance & regulatory requirements. The standard data retention policy is 180 days.

DATA REMOVAL

Rollbar removes sensitive data from electronic media, hardware, backups, and online storage per your compliance needs. This can be done in several ways, including destroying your encryption key or purging the data from the database.

DATA FILTERING

Rollbar libraries that integrate to your application's codebase are equipped with data filtering capabilities that allow you to filter out sensitive data prior to sending to Rollbar. Rest assured, even in cases where sensitive data is sent to Rollbar, the data is handled in a secure and compliant manner.

AUDIT CONTROLS

Rollbar Compliant SaaS maintains a comprehensive and auditable logs of activities. Examples include a list of all users and user activities associated with an account, and security logs of recent actions by any user in an account.

Compliance

HIPAA

Rollbar is fully compliant with HIPAA and the HITECH act. We have put in place all the required technical, physical, and administrative safeguards and passed the requisite audits.

As such, Rollbar Compliant SaaS is set up to receive sensitive data, including PHI and PII. As a matter of security best practice, we recommend filtering them prior to sending to Rollbar.

We will also sign a Business Associate Agreement (BAA) with each Rollbar Compliant SaaS customer as requested. For more info, see the BAA section.

ISO 27001

Rollbar is fully compliant with ISO 27001. We have implemented, are maintaining, and are continuously improving our information security management system (ISMS) in accordance with industry best practices.

CSA STAR

Rollbar is a registrant of Cloud Security Alliance's Security, Trust, and Assurance Registry (STAR). You can read Rollbar's CSA STAR Consensus Assessment Initiative Questionnaire at https://cloudsecurityalliance.org/star-registrant/rollbar-inc.

Data Centers

Our data centers are operated by Google as part of their Cloud Platform services. Our primary data center, where data is stored and encrypted at rest, is located in the Iowa region. We also utilize Google's points-of-presence network to deliver fast and reliable experience to users around the world.

Google Cloud Platform operates 11 regions and over 100 points of presence across the globe. It meets the industry's most stringent compliance standards, including AICPA SOC 1 / 2 / 3, PCI DSS, ISO 27001, ISO 27017, ISO 27018, HIPAA, CSA STAR, EU-US Privacy Shield, and My Number Act and FISC (Japan).

AICPA SOC 2 TYPE 2

AICPA SOC 2 certification concerns the internal controls in place at a third-party IT service provider organization, such as Google. It covers the security, processing integrity, and availability of the provider's systems, and the privacy and confidentiality of information maintained in those systems.

Our data center provider has achieved the stringent SOC 2 Type 2 certification, in which the systems, policies, and procedures in operation were evaluated for a minimum of six months.

Data Privacy

Rollbar complies with the EU-US Privacy Shield Principles and U.S.-Swiss Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access and enforcement.

Access to account data by Rollbar employees is limited to a necessary set of users consistent with their assigned Rollbar responsibilities, as per our 'need to know' and 'least privileged' policies.

As a Rollbar customer, you have control over what data is sent to Rollbar through the Rollbar libraries that integrate to your application's codebase.

You can filter out sensitive data prior to sending to Rollbar, such as for Payment Card Industry Data Security Standard (PCI / DSS) compliance purposes, or any other privacy concerns you may have.

Business Associate Agreement

Rollbar Compliant SaaS includes the option to have Rollbar sign a Business Associate Agreement (BAA) with you. The BAA is a contractual agreement that ensures Rollbar, as your business partner with access to PHI, is HIPAA-compliant.

SECURITY AWARENESS & TRAINING

Rollbar performs background checks, in compliance with local labor law and statutory regulations, on all soon-to-be-hired employees.

All Rollbar employees undergo security awareness training, upon initial hire and annually thereafter. The training curriculum includes security best practices and guidelines, and meets the mandated HIPAA training requirements.

PENETRATION TESTING

Rollbar undergoes third-party penetration tests on an annual basis. All items found in the testing are addressed, mitigated, or remediated depending on the severity of the finding. Summary reports are available to Rollbar Enterprise & Compliant SaaS customers.

Rollbar also commissions quarterly third-party vulnerability scans of our intellectual property space, and performs monthly internal vulnerability audits of our production environment.

We encourage outside security researchers to test the Rollbar application and report any vulnerabilities found to the Rollbar Security Team, in accordance with our Responsible Disclosure Policy. You can read it at https://rollbar.com/about/responsible-disclosure-policy.

Such testing shall be performed by account owners or authorized account members. We will respond and fix vulnerabilities in accordance with our commitment to security and privacy, and will not take legal action against or terminate access for those who discover and report security vulnerabilities.

INCIDENT REPORTING

One of Rollbar's top priorities is protecting the privacy of its customers. This is accomplished not only by proactively securing information, but also by handling and reporting incidents in a responsible, well-thought-out manner.

Rollbar has procedures in place for the handling and documentation of security incidents, the notification and limiting of incident exposure, as well as a response strategy to various security threats, including theft, denial of service, malicious code, and inappropriate use.

In the event of an incident, Rollbar will inform customers whose privacy has been compromised, after the information exposure has been confirmed.

CONTINGENCY PLAN

Rollbar has a Contingency Plan that establishes procedures to recover the Rollbar application quickly and effectively following a service disruption, as well as a Disaster Recovery Plan.

These plans are tested at least annually or when there is a major change in the Rollbar environment. Lessons learned from the tests are compiled and remediated by our Engineering team.

Per our backup policy, we also ensure accurate and current backups of production data are available for reconstitution after disasters or major anomalies.

More Information

SECURITY POLICIES

The following security policies can be made available for a customer review under a Non-Disclosure Agreement:

- Acceptable Use of Data in Test
- Access Control Policy
- Backup Policy
- Contingency Plan
- Device and Media Control Policy
- Encryption Policy
- HIPAA Data Retention Policy
- HIPAA Security Review Policy
- Information System Activity Review Policy
- Rollbar Vulnerability and Patch Management Policy
- Security Awareness and Training Policy
- Security Responsibility Assignment
- Software Development Life Cycle
- System and Information Integrity Policy

All policies are updated as needed and reviewed on an annual basis.

RISK MANAGEMENT

Our main goals in Risk Management are the continuation of the Rollbar service and the confidentiality, integrity, and availability of customer data.

We perform Risk Management on a regular basis and updates the Risk Management document as items progress. The official Risk Management document is reviewed and updated on an annual basis.

CONTACT US

Please read our online documentations at https://rollbar.com/docs/guides for more information on security features, and https://rollbar.com/docs/security for our compliance practices.

If you have any questions or require assistance, please contact our team at sales@rollbar.com.