Data Security Statement

Last Updated April 7, 2021

Ruby takes data protection very seriously. This Data Security Statement provides information about our security practices to give you confidence in how we secure the data you entrust to us. As an overall security measure, we make a point to not share too many details about our security practices. If you have specific questions not addressed in this Data Security Statement, please contact us at privacy@ruby.com.

This Data Security Statement is governed by and part of our Terms of Use. Any capitalized terms used but not defined have the meanings given them in the Terms of Use. In the event of any conflict between the Terms of Use and this Data Security Statement, this Data Security Statement shall govern with respect to the security measures in place to protect your data.

LEGAL AND REGULATORY STANDARDS

Ruby's dedication to your privacy and the security of your data is evident in our adherence to applicable legal and regulatory standards. We work hard to design our information systems and business processes to comply with:

- ***HIPAA.*** Ruby offers HIPAA-compliant receptionist and chat Services on a Customer opt-in basis. Our HIPAA-compliant Services make messages and other information available only via secure methods, such as our secure applications or online portal. Ruby only uses HIPAA-compliant service providers to serve our HIPAA opt-in Customers. Ruby will execute a Business Associate Agreement with HIPAA opt-in Customers.
- ***Privacy Laws.*** Ruby designs the Services to align with applicable privacy laws in the jurisdictions where we operate. Ruby's privacy practices include controls and procedures for Personal Information processing based on U.S. federal privacy laws, the California Consumer Privacy Act (CCPA) and other applicable state consumer privacy laws, the EU's General Data Protection Regulation (GDPR), and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Please see our Privacy Notice and Data Processing Agreement for detailed notices and other information related to these legal standards.
- ***PCI-DSS.*** Ruby's payment processing vendors are Payment Card Industry Data Security Standard (PCI-DSS) compliant.
- ***Cyber Insurance.*** Ruby maintains cyber insurance coverage.

DATA CENTER LOCATIONS

We store your data on Ruby's secure servers located in the United States. Ruby also hosts the Services and associated data on Amazon Web Services (AWS) and Opus, in both cases on servers located in the United States.

DATA SECURITY

Ruby implements reasonable and appropriate technical and organizational security procedures and practices to ensure a level of security appropriate to the level of risk of our processing. We follow industry best practices to protect your data from unauthorized or illegal access, destruction, use, modification, or disclosure. These practices include implementing security layers using both server authentication and data encryption to ensure that your data is safe, secure, and available only to authorized persons. Ruby maintains and adheres to comprehensive internal policies governing data security, physical security, network access, privacy, and confidentiality. All Ruby employees agree to our Confidentiality Agreement and internal policies governing privacy and data security.

ENCRYPTION

Ruby uses industry-standard encryption methods and products to protect your data in transit externally and at rest using TLS 1.2 & 1.3 with cipher suites using AES-128 & 256 and ChaCha20.

PASSWORDS

Ruby requires industry best practices around password requirements and storage. Furthermore, we require multi-factor authentication for all servers and third-party applications that contain Customer data.

NETWORK SECURITY

Ruby maintains a comprehensive approach to network security. Core servers and computers have industry standard anti-virus software installed, which is updated and continuously monitored to prevent unauthorized access to user data, network vulnerability scanning, network security monitoring, etc. Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network.

ACCESS CONTROL

Ruby follows the “Principle of Least Privilege”, with the intent of reducing access and only allowing employees and service providers access to the tools, systems, and data they need to perform their job. Access to production systems are role-based, centralized, auditable, and regularly reviewed. Access to Ruby’s network is only permitted through secure connectivity (e.g., VPN, SSH) and must be properly authenticated to access resources on our network.

LOGGING AND MONITORING

Ruby maintains and monitors audit logs on core servers and systems that store your data. Log information is stored to a centrally managed log repository for troubleshooting, security reviews, and analysis by authorized Ruby personnel. Logs are preserved in accordance with regulatory requirements. We will provide Customers with reasonable assistance and access to logs in the event of a security incident impacting their account.

BACKUPS

All networking components, load balancers, web servers, and application servers that are part of our Services are configured in a redundant configuration. Your data is stored on a primary database server that is clustered with a backup database server for redundancy and automatically backed up hourly or daily.

ASSET MANAGEMENT

Ruby maintains an asset management policy which includes identification, classification, retention, and disposal of information and assets. All company laptops are equipped with full hard disk encryption and up-to-date antivirus software and wiped per industry standards when decommissioned. Only devices meeting Ruby’s policy standards are permitted to access Ruby’s networks.

In addition to Ruby's own tools for protecting the network, Ruby leverages its service providers' respective data security safeguards. For example, AWS provides firewall rules and security groups which enable Ruby to secure its web, application and database servers.

CHANGE MANAGEMENT

All changes to Ruby's information systems or software follow Ruby's written change management process for infrastructure changes. Additionally, our proprietary applications are subject to a rigorous pre-release quality assurance and testing process, followed by a post-release verification testing and written process for communicating and tracking changes.

PHYSICAL SECURITY

Ruby implements sound physical and environmental security controls designed to reduce the risk of data compromise, physical failure of infrastructure components, damage from natural or fabricated environmental hazards, and access by unauthorized personnel. Our physical security controls include:

- Security camera monitoring 24 hours per day, 7 days per week.
- Access to premises is secured from unauthorized entry via personnel access credentials, visitor entry requirements, and visitor logs. All visitors are continually escorted by authorized staff.
- Hardware is stored in dedicated cages or similarly secured areas.
- Access to secure areas is limited to authorized personnel.
- Premises are designed to withstand adverse weather and other reasonably predictable natural conditions.

In addition to Ruby's own physical security measures, our information systems infrastructure (servers, networking equipment, etc.) hosted by AWS and Opus Interactive are secured by physical security measures designed to provide physical data security and formal physical access procedures.

For more information on AWS physical security see AWS's website.

For more information on Opus Interactive physical security see the Opus Interactive website.

HUMAN RESOURCE SECURITY

Ruby's employees play a critical role in designing, developing, implementing, and securing Ruby's information systems. Ruby has designed a comprehensive program to train, inform, and structure job duties in a manner that best support's the company's commitment to data security, including:

- ***Employee Policies.*** Ruby communicates its information security policies to all employees and contractors. Ruby's information security policies are found in the Employee Handbook and include, without limitation, policies governing physical security, data security, acceptable use, remote access, wireless devices, software download and installation, and data classification and handling. Ruby maintains and regularly reviews and updates its information security policies, at least on an annual basis. Employees must read, agree to, and follow these policies. All new employees are required to sign the company's confidentiality agreement.
- ***Security Personnel.*** Ruby employs a cross-functional project team that meets regularly to develop and manage security and privacy programs and projects. The team addresses network, application, and system security, as well as incident management procedure.
- ***Security Training.*** All new Ruby employees and contractors attend security training during the on-boarding process. Ruby requires employees to complete security training such as HIPAA

training, security awareness training, and job specific security and skills development and/or privacy law training for key job functions. Training is required at least annually and is scheduled and designed to adhere to all specifications and regulations applicable to Ruby. Training is tracked and monitored for compliance.

VULNERABILITY MANAGEMENT

Ruby uses several sources and tools to identify, track, respond to, and remediate network vulnerabilities, including:

- **Organizational Security.** We maintain and monitor notifications, errors, logs and alerts on our Services, and from all systems to identify and manage threats. We also maintain internal information security policies, including incident response plans.
- **Patch Management**. Patches and upgrades are deployed to clusters of servers and systems in a staggered manner to ensure all services remain uninterrupted during the application of patches or upgrades. Patches are applied based on the severity level of the vulnerability according to our patch management guidelines.
- **Vulnerability Disclosure.** If you identify a vulnerability in our Services, you can report it to privacy@ruby.com.

SECURITY INCIDENT RESPONSE

Ruby maintains a Security Incident Response Plan (SIRP). The SIRP includes protocols to prepare for incidents via prevention, training, and resources standards, detect and analyze incidents using a multistep process to prioritize and respond to the incident through the recovery stage, and completing post-incident meetings and corrective actions. Our breach notification procedures are consistent with our obligations under applicable country, state and federal laws and regulations, as well as any industry rules or standards applicable to us. Ruby will promptly notify a Customer in the event Ruby becomes aware of an actual or reasonably suspected Security Incident involving the Customer's data.

DATA DELETION

Upon termination or expiration of a Customer's agreement with Ruby, we will delete, anonymize, or return all Customer Data (as defined in the Data Processing Agreement) that we Processed as part of the Services in accordance with the Customer's reasonable Instructions. Ruby reserves the right to retain certain Customer Data in compliance with applicable legal and contractual exceptions and limitations.

THIRD PARTY SERVICE PROVIDERS

Ruby maintains and follows a Third Party Service Providers/Vendors Policy to ensure that Ruby's Third Party Service Providers ("TPSPs") are able to maintain the privacy, confidentiality, security, integrity, or availability of your data consistent with our contractual obligations to our Customers. Ruby performs due diligence on each TPSP prior to engagement, including review of relevant compliance standards (e.g. HIPAA, PCI, CCPA, GDPR, and data security certifications). Ruby obtains contractual commitments from each TPSP to maintain adequate safeguards around your data consistent with our own contractual obligations to our Customers.

BUSINESS CONTINUITY AND DISASTER RECOVERY

Ruby maintains a formal Business Continuity and Disaster Recovery Plan applicable to all systems where your data is stored. Our Plan addresses geographic availability, multiple site availability, and replication of critical systems and data in the event of a number of different disaster scenarios. We perform regular recovery testing. We also require our service provider’s data centers to have adequate disaster recovery plans.

YOUR DATA SECURITY

Keeping your data safe also depends on you ensuring that you preserve the security of your account, systems and data. You should ensure that you have sufficient security on your own systems and use sufficiently complicated passwords and store them safely. For more information on securing your data with Ruby, please review our Privacy Notice.

CHANGES

Ruby reserves the right to amend this Data Security Statement at any time. Any material changes will be posted on this page. Continuing to use our Services after we post changes means you accept those changes.