RChilli Security - Data Privacy

RChilli Provides dedicated process to implement data security of all content hit to our servers / shared with us.

Following bullet points are listed for reference. Detailed process is listed in our Server section maintained internally. Please note for security purpose we cannot share complete internal points over here.

Physical security

RChilli Development center is under security protection. Internal Office is under security camera surveillance.

All critical servers/infrastructure is under digital and physical locks where it maintains access control and strict password control.

RChilli hosts its application and data in industry-leading hosting companies of repute. We keep either of following hosting providers Amazon Web Services, Softlayer, Rackspace, or Gogrid. Data centers have been thoroughly tested for security, availability and business continuity.

Application security

To ensure application security, we take a multifaceted approach to ensure everything from engineering to deployment, including architecture and quality assurance processes complies with our highest standards of security.

Application Architecture

RChilli Application is packed with 4-layer architecture formula, comprises of Firewall, Load Balancer, Application, and Database. Everything is so distributed that user cannot touch database without reaching to any of internal servers.

RChilli uses a multi-tenant data model to host all its applications. Each application is serviced from an individual virtual private cloud and each customer is uniquely identified by a tenant ID. The application is engineered in a way that each user gets its own folder or server. No point requests are shared with same instance. Per this design, no customer has access to another customer's data. Access to the application by the RChilli development team is also controlled, managed and audited. Access to the application and the infrastructure are logged for subsequent audits.

Quality Assurance

Besides functional validation and verification, the quality assurance process at RChilli also subjects application updates to a thorough security validation. The validation process is performed by a dedicated app security team with ethical hackers whose goal is to discover and demonstrate vulnerabilities in the application. An update to the application does not get the stamp of approval from the quality assurance team if vulnerabilities (that can compromise either the application or data) are identified.

Deployment & Post Deployment

Deployments to production servers are performed only by trusted and authorized engineers. Only very few pre-authorized engineers have access to RChilli's production environment. To view and inspect access logs, engineers need to go through a committee of authorized employees, who will then deliver the logs to them after validating their purpose.

Data Security

RChilli takes the protection and security of its customers' data very seriously. RChilli manages the security of its application and customers' data. However, provision and and access management of individual accounts is at the discretion of businesses that own them.

Our products collect very limited information about customers - name, email address and phone - which are retained for account creation. Postal address is requested and retained by RChilli PCI compliant payment processor for billing.

For Resumes content we only save, date and time, IP address, File name, User key, Sub User ID, count of resume pages, time taken to process. No other information is stored unless explicit request is made in writing.

RChilli takes the integrity and protection of customers' data very seriously. We maintain history of two kinds of data: application logs from the system, and application and customers' data. All data is stored.

Different environments are in use for development and testing purposes, and production. At the moment, RChilli does not have any information classification scheme, but work is in progress towards its implementation.

Operational Security

RChilli understands that formal procedures, controls and well-defined responsibilities need to be in place to ensure continued data security and integrity. The company has clear change management processes, logging and monitoring procedures, and fallback mechanisms which have been set up as part of its operational security directives. An information security committee is present to oversee and approve all organization-wide security policies.

Operational security starts right from recruiting an engineer to training and auditing their work products. The recruitment process includes standard background verification checks on all new recruits. All employees are provided with adequate training about the information security policies of the company and are required to sign that they have read and understood the company's security-related policies. Confidential information about the company is available for access only to select authorized RChilli employees.

Employees are required to report any observed suspicious activities or threats. The human resources team takes appropriate disciplinary action against employees who violate organizational security policies.

Only authorized and licensed software products are installed by employees. No third parties or contractors manage software or information facilities, and no development activity is outsourced. All employee information systems are authorized by the management before they are installed or used.

Network Security

Network security is discussed in detail in this section from the perspective of the development center, and the network where the application is hosted.

The RChilli office network where updates are developed, deployed, monitored and managed is secured by industry-grade firewalls and antivirus software, to protect internal information systems from intrusion and to provide active alerts in the event of a threat or an incident. Firewall logs are stored and reviewed periodically. Access to the production environment is via SSH and remote access is possible only via the office network. Audit logs are generated for each remote user session and reviewed. Also, the access to production systems are always through a multi-factor authentication mechanism.

Regulatory Compliance

All formal processes and security standards at RChilli are designed to meet regulations at the industry, state, federal and international levels. RChilli adheres to strict data security, access, integrity policies, among other principles defined in the safe harbor framework. The third-party payment processor used by RChilli is PCI compliant, meaning credit card data is securely stored and processed.

Use of our service by customers in the European Economic Area ("EEA"), will include the processing of information relating to their customers. In providing our service, we do not own, control or direct the use of the information stored or processed on our platform at the direction of our customers, and in fact we are largely unaware of what information is being stored on our platform and only access such information as reasonably necessary to provide the service (including to respond to support requests), as otherwise authorized by our customers or as required by law. We are the data processors and not the data controllers of the information on our platform for purposes of the European Union ("EU") Directive 95/46/EC on Data Protection ("EU Directive") and the Swiss Federal Act on Data Protection. Our EEA or Switzerland based customers, who control their customer data and send it to RChilli for processing, are the "controllers" of that data and are responsible for compliance with the Directive. In particular, RChilli's customers are responsible for complying with the Directive and relevant data protection legislation in the relevant EEA member state before sending personal information to RChilli for processing.

Reporting issues and threats

If you have found any issues or flaws impacting the data security or privacy of RChilli users, please write to support@rchilli.com with the relevant information so we can get working on it right away.

Your request will be looked into immediately. We might ask for your guidance in identifying or replicating the issue and understanding any means to resolving the threat right away.

Please be clear and specific about any information you give us. We deeply appreciate your help in detecting and fixing flaws in RChilli, and will acknowledge your contribution to the world once the threat is resolved.

Get in touch with us

If you have any questions or doubts, feel free to get in touch with us at support@rchilli.com, and we'll get back to you right away.