RollKall

RollKall Data Security Overview

RollKall has the highest uptime and performance rates in the industry.

Guaranteed Uptime 99.95%

Setting High Standards for Optimal Data Protection

RollKall adheres to high security measures to ensure our system and your data are secure. Through our Azure infrastructure, RollKall includes the following best practices to ensure proper safeguarding of our clients' data from unauthorized access, destruction, use, modification, or disclosure.

- Features such as encryption, Structured Query Language (SQL) threat detection, firewall rules, and data masking, to ensure proper safeguarding of our client data.
- Active Directory (AD) authentication and authorization enable identity management of database users and other Microsoft services in one central location.
- Cloud-first application with no physical servers; all RollKall infrastructure is hosted on Microsoft's Azure platform and in multiple geo-redundant locations in the continental U.S. RollKall's primary hosting location is in the North Central US service region, located in Illinois.
- Multi-tenant environment, with off-duty shifts and user accounts in a shared database environment that allows for segregation of sensitive client data. Each client's data is segregated through the proper implementation of user permissions and roles for each organization.
- Security/privacy policies and procedures are in place and reviewed regularly.
- SQL database provides tracking of database events and creates an audit log to record events in an Azure storage account.
- Penetration and vulnerability tests are performed quarterly.
- PCI audits are performed quarterly.
- Backups of the RollKall system are performed daily and are stored within Azure.
- Payments are processed through Stripe, a third-party PCI-certified, Level 1 Service Provider.
- RollKall's cyber insurance policy provides additional assurance in the event of a data security breach.

Could you please detail RollKall's practices related to features such as encryption, SQL threat detection, firewall rules, and data masking?

RollKall's infrastructure follows best practices to properly safeguard all user data, including:

- FIPS 140-2 approved encryption methods. During transit, the data is encrypted using TLS 1.2. Always Encrypted Columns ensure that sensitive personal data never appears as plain text inside the database system.
- Azure SQL Database is configured to use Transparent Data Encryption (TDE), which performs real-time encryption and decryption of the database, associated backups, and transaction log files to protect information at rest. TDE provides assurance that stored personal data has not been subject to unauthorized access.
- SQL Threat Detection enables the detection and response to potential threats as they occur by providing security alerts for suspicious database activities, potential vulnerabilities, SQL injection attacks, and anomalous database access patterns.
- Firewall rules prevent all access to database servers until proper permissions are granted. The firewall grants access to databases based on the originating IP address of each request.
- SQL Database Dynamic Data Masking (DDM) limits sensitive personal data exposure by masking the data to non-privileged users or applications.
- RollKall's strict security measures meet PCI-DSS compliance standards. Our latest certificate of compliance is available upon request.

Does RollKall have independent attestations such as PCI- DSS, or related certificates?

Yes. RollKall is PCI-DSS compliant. RollKall performs quarterly PCI scans to ensure our API and Portals are PCI-DSS compliant. The certificate from our most recent PCI scan is available upon request.

Does RollKall accept credit cards? If so, can RollKall show it is PCI compliant at all times?

Yes. RollKall payments are processed through Stripe, a third-party PCI-certified, Level 1 Service Provider. Additionally, RollKall performs quarterly PCI scans to ensure our API and Portals are PCI-DSS compliant. The certificate from our most recent PCI scan is available upon request.

Could you please describe RollKall's security around logins and passwords?

- The application will enforce password complexity. At account creation, we ensure that the user's password is not composed of common phrases or a password that can be easily guessed by an attacker.
- Application users can request a password reset OR change their current password while logged in.
- The application will throttle login attempts and temporarily lock a user account if too many failed attempts are detected. These lockouts are temporary, and after a period of time, the platform will be unlocked again for the user.

Could you provide a high-level overview of how RollKall limits access to your Azure SQL Database through firewall rules?

Access to the RollKall system is limited to whitelisted IP addresses using the SQL Server Firewall. We use Azure AD Authentication with multi-factor authentication, with dynamic data masking to protect sensitive data. Any access to the database for deployment or development purposes has to be made through a VPN connection.

How often does RollKall perform code reviews in your program?

RollKall's current development process includes code reviews for every feature/bug that will be merged into our main development branch.

How will RollKall access the agency's data? *Example: Is the data supposed to be sent to your organization via email or will the data need to be uploaded to an application?

We collect minimal PII required to verify that a user is an active law enforcement employee. Data provided to our application will be entered by the users themselves (regarding any PII or off-duty data) through our web or native interfaces. RollKall does not share officer data with unrelated parties. Your officer and agency information is secure.

How frequently does RollKall update your software? What is the client/vendor notification process?

RollKall's current release schedule adheres to a production release every 4 weeks for both the Mobile Application and the Web Portals. Each release is accompanied by proper communications to the user base via multiple supporting materials that include: 1) email communications to inform the users of the new features available, 2) detailed release notes with the issues and features included on the release, and 3) training videos demonstrating and educating on the proper use of the new features.

Could you provide a high-level overview of RollKall's Security Software Development Life Cycle (SSDLC) practices?

RollKall adheres to the Agile Scrum secure software development process with 2-week sprints and monthly releases. This allows for continuous product improvement and flexibility in meeting our users' needs.

Our internal Product Team plans and prioritizes feature requests. Stories are generated and groomed in conjunction with the internal Engineering Team. Once stories are ready, they are onboarded into a sprint in which development is done according to the specs.

Every feature or bug goes through a peer code review process, ensuring code adheres to our best practices and standards. At the end of the sprint, every story goes through a quality assurance certification process by our internal Quality Assurance Team who ensure the stories adhere to specs and do not cause any regressions. Once Quality Assurance certifies a build and the features are accepted by our Product Team, it will be released into production, along with any supporting material and communications for our internal and external stakeholders.

Does RollKall have a direct number or help desk for reporting system bugs or program-related problems? What is the normal response time?

Yes. Support requests are handled through RollKall's dedicated Customer Experience Team that takes incoming requests via phone, email, or the app's help menu, each of which will open a support ticket. All tickets and communications are handled internally through Zendesk.

Response time is determined by several factors including urgency (whether work can still be completed), impact (how many people it affects), and severity (the type of error). For example, urgent, high-impact, severe tickets are typically resolved within an hour, but can also depend on the time required to resolve the issue. Lower priority tickets typically take 12-48 hours but may take longer if product design is required.

Describe any downtime experienced by RollKall during the last 12 months when services were not made available.

RollKall has had an uptime/availability percentage of 99.98% in the last year. Downtime has only been experienced for brief moments during scheduled deployments of new features.

The only unplanned outage we have suffered in the last year was April 1st, 2021, when Microsoft Azure had intermittent outages related to their DNS, which caused our application to be unavailable in parts of the country for about 30 minutes.

What happens if there is a data breach?

We live in a world where cyber-attacks are a real threat, and nobody is immune. RollKall carries a $1Million (per occurrence) cyber insurance policy to further protect your data, which covers:

- Notification to officers and clients affected
- Assistance with the restoration of personal identities of affected officers
- Recovering compromised data
- Payment for credit monitoring services

Describe RollKall's Disaster Recovery (DR) and continuity of operations plan.

RollKall is a SaaS application hosted in Microsoft Azure as such our Disaster Recovery plans are implemented using Azure best practices for a resilient infrastructure. Our current DR plans include the following.

- App Services - Automatic failovers happen to the secondary region in case of primary region failure.
- SQL DB – Geo-Replication with read replica in a secondary region with manual failover
- Azure Storage – In Geo-Redundant replication mode