RockStep

SOLUTIONS POWERING RESEARCH

SECURITY AND PRIVACY WHITEPAPER

SECURITY AND PRIVACY WHITEPAPER

INTRODUCTION

We at RockStep Solutions recognize the importance of security and privacy and have built multiple protective layers for our customer's data, software development process, and company operations. These protections are described herein.

Climb is a flexible, mobile friendly animal colony management and laboratory workflow management product that supports scientific research. Only authenticated users have access to the Climb application and API layer, and are restricted to viewing only those data associated with their workgroup. Climb makes use of automated data audit logging, providing an audit trail for all data changes in support of regulatory compliance.

The Climb application is hosted on a cloud server infrastructure managed by a world class hosting provider (Microsoft Azure [1]). Both technicians and researchers use Climb via an HTML5 compliant web browser with Internet connectivity.

Because of the proprietary and sensitive nature of the research data being managed by Climb, we consider the confidentiality of our customer's data within Climb to be of the utmost importance. Therefore, we have designed and developed Climb with privacy and security in mind from the ground up.

Our commitment to protecting data is underscored by our “personal stake” in the software. Employees at RockStep Solutions undergo regular training about safeguarding data. We also put significant resources into reviewing and improving the security and privacy of Climb system components so we can maintain the high level of trust that our clients and customers expect.

[1] https://azure.microsoft.com/en-us/support/trust-center/

DATA CENTER

RockStep Solutions partners with Microsoft Azure to provide a secure and reliable server infrastructure and resource management service. Azure has achieved ISO 27001 certification and has been validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). Azure has passed annual SOC 1 and SOC 2 audits as well as FDA 21 CFR Part 11 and FedRAMP. See the Azure Qualification Guideline for more detailed information[2].

Azure facilities include the following features:

- Highly secure data centers utilize state-of-the art electronic surveillance and multi-factor access control systems.
- All data centers are staffed by trained security guards 24x7x365
- Access to data centers is authorized on a least privileged basis
- Environmental systems are designed to minimize disruptions to operations

SERVICE UPTIME AND DISASTER RECOVERY

Azure provides backup and recovery services, including geo-replication, which provides redundancy of data across regions to ensure access to data in the event of a local disaster. Backups are stored in encrypted format. The Azure platform is proven to have 99.95% compute availability and 99.9% storage and database availability. Automated database backups allow point in time restore to within 15 minute intervals going back 30 days. Standard recovery point objective (RPO) for a geo-redundant Azure SQL database is 1 hour.

In the event of hardware failure, affected resources are automatically moved to new hardware. Hardware failure does not cause service interruptions. Fault tolerance is built into the Climb application, long running operations are idempotent to avoid orphaned or corrupt data if a failure occurs during a transaction. Climb employs a fault detection/retry strategy for data retrieval and saving.

Application resources, including web applications, databases, and file storage are monitored constantly for performance and availability using Azure's Application Insights instrumentation service. Should there be a sudden rise in failure rates or if abnormal performance patterns emerge, the RockStep technical team is alerted so that the issue can be resolved as quickly as possible.

In the eleven months Climb has been live in production, there have been three instances of system outages, each lasting less than one half hour and neither resulting in any customer data loss.

[2] https://azure.microsoft.com/en-us/support/trust-center/compliance/

APPLICATION SECURITY FEATURES

Climb provides the following security features:

- **Workgroup Segregation of Data** – Each Climb workgroup is provisioned with a standalone database containing only that workgroup's data. Users login within the context of a workgroup and requests for data are routed to the appropriate schema.
- **Login Event Tracking -** All login events, including failed logins, are recorded and available for auditing.
- **Audit Logging –** Every change to Climb data is recorded in history tables within the Climb database, allowing users to view a history of values along with who changed the values and when the change occurred.
- **Authenticated Data Access –** All access to Climb data is via a secure OData Web API layer that is compliant with the OAuth security protocol. All API requests require an authentication token header, which is available only by authenticating through Climb login.
- **Encrypted data** – The Climb application is only accessed via secure protocol, so data transmitted between the Climb database and the browser are encrypted via the SSL security protocol. Climb data are encrypted at rest in the Climb Azure SQL database using Azure's Transparent Data Encryption protocol (TDE.) TDE performs page level encryption of the data before it is stored and decryption of the data as it is read into memory. All files uploaded into Climb are stored in encrypted format.
- **Role based security** – Climb allows administrative users to define workgroup roles. Every user is assigned to a role. Each role may be configured to have a custom set of access privileges to application functionality. A role has no access, read only access, or read/write access to each set of application functionality.

SECURE DEVELOPMENT PRACTICES

Standard security practices for web based applications are used, including:

- Input validation (expected data types, data range and length)
- Least privilege approach, restrict users to only the functionality and data that is required to perform their tasks
- Authentication for all requests to all resources
- Centralized authentication control
- Storage of cryptographically strong hashes of passwords
- Change of all vendor-supplied or default passwords
- Restricted access to database servers with IP firewall rules managed only by the Azure system administrator
- Encoding of hazardous characters
- Escaping output (preventing XSS attacks)
- Code reviews on all application code prior to check in. Code is peer reviewed quality and security vulnerabilities. No code is merged into the main repository without peer review.
- Every software build and release is tracked and archived.

COMPANY POLICIES

RockStep Solutions maintains and enforces policies that provide a thorough and structured approach to security within our organization. These policies include:

- All employees and contractors are required to execute a non-disclosure agreement
- Access to company resources is controlled by Active Directory and based on individual account logins and security group membership
- RockStep Solutions leverages LastPass password management software to enforce password policies for uniqueness, strength, and periodic changing. RockStep controls password sharing through LastPass and requires changing of shared passwords upon termination of any employee
- Access to customer information, when necessary, follows a “just in time access” approach, wherein the employee accesses the data for a limited time and for a specific purpose such as troubleshooting
- Secure computing methods for workforce members that access sensitive information (vulnerability education, hard drive encryption, malicious software protection)
- Quarterly risk and vulnerability reports
- Emergency contingency plans (e.g., loss of key employees)
- Annual company-wide security and privacy training
- Annual security reviews by independent 3rd-party experts

APPENDIX 1: FAQ

Q: What is your uptime policy or SLA (service level agreement)?

Unless otherwise noted, the Climb application runs 24x7x365. We reserve short, regular maintenance windows, outside of normal business hours, where software updates can be performed. Users are notified in advance of maintenance windows.

Q: What happens when a security vulnerability is discovered?

Operating system security patches are deployed through our Azure platform SLA and do not result in system interruption. We employ a responsible disclosure policy for application security vulnerabilities, and our automated deployment pipeline allows rapid release cycles. RockStep follows a "roll forward" release policy, as soon as vulnerabilities are discovered, an updated version of the software addressing the vulnerability is released.

Q: What is the administrative procedure for creating a new account? How are forgotten passwords reset?

Climb accounts are created in a self-service fashion. Anyone may create a Climb account. Administrators manage registration codes, which allow users to register directly into a workgroup and role. Climb offers self-service password reset. Passwords (or any other form of login credentials) are never sent by email.

Q. Are cookies used to track the client's navigation of the Climb software or external resources?

Climb collects various statistical parameters during a user's visit. These data are related only to application health and performance and are not linked back to individual user accounts. No external resource access is tracked.

Q: What software, languages, frameworks, etc. does Climb use? How is Climb architected?

Please see Appendix 3: Software Stack and Appendix 4: System Architecture

APPENDIX 2: PROTECTED INFORMATION

Climb stores and uses the following information for each user:

- User ID
- Password
- User name
- Email addresses (optional)
- Telephone numbers (optional)

APPENDIX 3: SOFTWARE STACK

APPENDIX 4: SYSTEM ARCHITECTURE