Molecule Software, Inc.
Data Security Addendum

This Data Security Addendum ("Addendum") describes the administrative, technical, and physical controls applicable to the Molecule Service provided under the Subscription Service Agreement ("Agreement"). Capitalized terms not defined in this Addendum have the meanings set forth in the Agreement.

APPLICATION SECURITY

SDLC

Molecule maintains Software Development Life Cycle (SDLC) policies that govern the design and implementation of application and infrastructure changes.

Quality assurance (QA) and code review processes maintain standards for product quality, security and user experience.

Version Control and Patching

Our application codebase is version-controlled,main branches are protected, and changes to the codebase are subject to comprehensive CI tests, code reviews, QA cycles, and approvals. Changes made to the application codebase are tracked and history is maintained in version control.

Molecule's patch management policy ensures that operating systems, software, frameworks, and libraries used in Molecule's infrastructure are updated on a regular basis.

Secrets Management

Application secrets are managed through using a secure Vault. Access is restricted to applicable engineers.

Tokens, passwords, certificates, and other sensitive data are securely stored in encrypted form. Access and usage of application secrets are regularly audited and monitored.

ACCOUNT SECURITY

Login and Sign Up

Authentication in Molecule is enforced with industry-leading libraries and providers. Molecule uses Okta's Auth0 to support web authentication. Customers can opt to manage user access through single sign-on (SSO) authentication using an external identity provider or via user-configured passwords. For fallback purposes, Molecule also supports authentication using magic links.

Sign-in is configurable with an option to turn on two-factor authentication.

Password and Sessions

User passwords are managed by an external identity provider. More information about Okta's security policies can be found here.

Sessions on Molecule have a finite duration.

Molecule employs user cool-down and lock-out functionality. The Molecule team can also lock out a user upon request.

Customer and Account Permissions
Position and market data are tagged with an account ID so that users can only access data that belongs to their account. Every release is tested by our team to ensure users see only what they are authorized to see.

User and Group Permissions
An account administrator can grant permissions to govern the actions users can perform in the system and the screens and types of data that users can see. This can also be done at a custom group level.

API Permissions
API access requires a username and token. These tokens are one-way encrypted and revokable.

Access Logs
Molecule retains access logs of application usage and can make them available upon request while retained in the Service.

INFRASTRUCTURE SECURITY

Physical AWS security
Molecule uses AWS as its primary cloud hosting provider. AWS handles the physical security of the facilities in which the services operate in addition to the security of the host operating system and virtualization layer. More information can be found here.

Network Security
Molecule has defined strict network security rules. Only the portions of the application we specify are available outside the data center.

Communication within the data center is secured by Amazon's network security systems. More information can be found here.

Staging Environment
Molecule has a dedicated staging environment isolated from our production environment with separate access policies. Changes made to the infrastructure/application are first deployed and tested in the staging environment before rolling it out to production.

Production Access
To access our production environment, engineers are required to use a VPN which establishes a secure connection between the AWS network and endpoint device. More information can be found here.

Access to the AWS Console is restricted to a limited group of engineers and is given on a need-to-know basis.

DATA SECURITY

Multi-tenant Architecture

Molecule is built as a multi-tenant SaaS application. At the data layer, all customer accounts are logically isolated.

Testing on Every Major Release
Molecule employs an array of testing techniques including linting, static code scans, peer review, manual testing, 90%+ coverage ratio for automated tests and post-release security testing.

Automated testing ensures that account security is maintained as features are added and changed.

Encryption at Rest and in Transit
Customer data is stored within AWS and encrypted at rest, providing an added layer of security. Customer data is encrypted in transit using the Transport Layer Security (TLS) protocol. Insecure protocols, such as HTTP, are either redirected to HTTPS or blocked using AWS security groups.

ENDPOINT SECURITY

Devices Are Encrypted and Managed by MDM
A Mobile Device Management (MDM) solution automatically installs security components and allows Molecule to remotely wipe devices if they are compromised. The MDM system also enforces security patching from Apple and Windows.

Employees who have access to our production infrastructure and data are required to have anti-malware applications installed on their systems.

SOC COMPLIANCE

Molecule meets the standards of AICPA SOC 1 Type II and SOC 2 Type II and is audited annually to ensure continuing compliance.