Data Innovations LLC
Security Measures

Data Innovations ("DI") currently abides by the security standards ("Security Measures") set forth herein in the provision of subscription services ("Subscription "Services") to its customers pursuant to a separate underlying subscription services agreement ("Subscription Services Agreement"). DI may update or modify these Security Measures from time to time provided such updates and modifications win not result in a degradation of the overall security of the Subscription Services during the applicable Subscription Services Term.

DI Platform. DI use certain computer software applications, tools, APIs, connectors, programs, networks and equipment to make the Subscription Services and certain applications available to Customer on an internet-hosted infrastructure.

Hosting Infrastructure. DI hosts its Subscription Services in geographically distributed, secure data centers operated by Amazon Web Services ("AWS")*.

Redundancy. The Subscription Services are replicated across multiple availability zones (data centers) within a geographic region to eliminate single points of failure in order to minimize the impact of environmental risks.

Monitoring. The Subscription Services are protected by monitoring which is designed to detect a variety of failure conditions and which will, when appropriate, trigger scaling and/or failover mechanisms.

Backups. Backups of the DI Platform and any data contained therein are performed on a regular basis and replicated to multiple availability zones (data centers).

Business Continuity. DI replicates its Subscription Service and data over multiple availability zones (data centers) within a geographic region to protect against loss of the Subscription Service. DI conducts periodic tests of failover and data backup procedures to ensure readiness for business continuity and disaster recovery.

Networks & Transmission.

- Network Security. DI has multiple layers of denial of service protection, intrusion rate limiting and other network security services from both its hosting and third-party providers.
- Encryption Technologies. DI requires HTTPS encryption (also referred to as SSL or TLS connection) for all external data transfer.

Policies and Procedures.

- DI has written, approved policies and procedures governing account management, acceptable use, data retention, employee code of conduct, encryption, incident response, information security, use of mobile devices, password protection, patch management, risk management, data breach notification, change management, communication, disaster recovery, system backup and recovery, and monitoring.

Security Response. DI monitors a variety of communication channels for security incidents, and DI's security personnel are required to react promptly to known incidents.

Access Controls.

- Access Procedures. DI maintains formal access procedures for allowing its personnel access to the production environment and components involved in the production environment. Only authorized employees are allowed access to these restricted components. Only a small number of individuals are approved to access the restricted components. Audit records are maintained to indicate who has access to restricted components.
- Access Mechanisms. Access to DI's production service and build infrastructure occurs only over a secured channel and requires two-factor authentication.

Logging. Access to DI's production environment and build infrastructure is done using unique IDs and is logged.

Infrastructure Security Personnel. DI maintains several security policies governing its personnel. DI's infrastructure security personnel are responsible for the ongoing monitoring of DI's security infrastructure, the review of the production environment, and responding to security incidents.

Data Protection.

- In Transit. Interactions between users, administrators and DI modules are done using the Secure Socket Layer ("SSL") or Transport Layer Security ("TLS") standard cryptographic protocols enforcing a minimum TLS version of 1.2.
- At Rest. DI uses cryptographic hashing and encryption mechanisms to protect sensitive information such as cryptographic keys and application secrets.
- Redundancy. The DI stores data in a multi-tenant environment within DI's hosted infrastructure. The data and Subscription Services are replicated across multiple hosted datacenters within the same geographic region.

Data Isolation. DI logically isolates the customer's data, and the customer has a large degree of control over the specific data stored in the Subscription Services.

Security Scan. DI employs a third party to scan the source code of any applications on the DI Platform and perform penetration testing for security vulnerabilities on a periodic basis.

Good Development Practices. DI has defined practices that follow industry standards and includes a well-documented Quality Management System.