Information Security Controls and Technical and Organizational Measures over Condor's Software

The following sections define Condor's information security controls and technical and organizational measures to protect Client Data and are incorporated into this Agreement.

1. PHYSICAL ACCESS CONTROL

- Condor has architected its systems to eliminate physical access or security risk, given the Software is a cloud-based installation hosted by Amazon Web Services (AWS).

2. SYSTEM ACCESS CONTROL

Data processing systems used to provide the Software are prevented from being used without authorization by taking the following measures:

- Multi-factor authentication is required to access the production environment.
- All personnel access Condor's systems with a unique identifier (user ID).
- Condor has procedures in place that require user access to be granted only with proper authorization. Upon separation, user access rights are revoked in a timely manner.
- Condor has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form.
- Access control lists on production application and database security groups are configured to deny all inbound connections unless from the load balancers or other authorized sources.
- Condor uses up–to-date antivirus software on laptops and workstations that have access to sensitive information.
- Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to Condor's corporate network and critical infrastructure is protected by strong authentication.

3. DATA ACCESS CONTROL

Persons entitled to use data processing systems gain access only to the Client Data that they have a right to access, and Client Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage. Condor takes the following measures:

- As part of the Condor Security Policy, Client Data requires at least the same protection level as "confidential" information according to the Condor Information Classification standard.
- Access to Client Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfill their duty. Condor uses authorization concepts that document grant processes and assigned roles per account (user ID). All Client Data is protected in accordance with the Condor Security Policy.
- A Condor security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

4. DATA TRANSMISSION CONTROL

Except as necessary for the provision of the Software in accordance with the Agreement, Client Data will not be read, copied, modified or removed without authorization during transfer. Condor takes the following measures:

- Client Data transferred over Condor internal networks is protected according to Condor Security Policy.
- The Software utilizes Transport Layer Security (TLS) v1.2 (or above) and Hypertext Transport Protocol Secure (HTTPS) to encrypt data during transmission.

5. DATA INPUT CONTROL

It will be possible to retrospectively examine and establish whether and by whom Client Data have been entered, modified or removed from Condor data processing systems. Condor takes the following measures:

- Condor only allows authorized personnel to access Client Data as required in the course of their duty.
- Condor has implemented a system to log input, modification, or deletion of Client Data within the Software to the extent technically possible.

6. PERSONNEL CONTROL

Client Data being processed on commission (i.e., Client Data processed on a customer's behalf) is processed solely in accordance with the Agreement and related instructions of the customer. Condor takes the following measures:

- Condor uses controls and processes to monitor compliance with contracts between Condor and its customers, subprocessors or other service providers.
- As part of the Condor Security Policy, Client Data requires at least the same protection level as "confidential" information according to the Condor Information Classification standard.
- All Condor employees and contractual or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of Condor customers and partners.

7. AVAILABILITY CONTROL

Client Data will be protected against accidental or unauthorized destruction or loss. Condor employs regular backup processes to provide restoration of business-critical systems as and when necessary. Condor takes the following measures:

- Condor has configured its cloud systems to run on multiple availability zones for redundancy in case of system failure.
- The production environment is monitored through various tools. Alerts are configured to notify responsible personnel at predefined degradation thresholds related to performance and processing capacity. Critical and high-risk items are tracked through resolution.

8. DATA SEPARATION CONTROL

Client Data collected for different purposes can be processed separately. Condor takes the following measures:

- Condor uses the technical capabilities of the deployed software (for example: multi- tenancy, or separate system landscapes) to achieve data separation among customer data originating from multiple customers.
- Customers only have access to their own data.

9. DATA INTEGRITY CONTROL

Client Data will remain intact, complete and current during processing activities. Condor takes the following measures:

- Condor has implemented a multi-layered defense strategy as a protection against unauthorized modifications.
- In particular, Condor uses the following to implement the control and measure sections described above:
    - Security Group / Load Balancers restrictions
    - Data encryption at rest and in transit
    - Restriction of access to production to only authorized personnel
    - Multi-factor authentication controls
    - Antivirus software
    - Production data logging and monitoring
    - External and internal penetration testing
    - Regular internal audits to prove security measures