Data Security Policy

LangChain maintains a comprehensive, written information security program that contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of LangChain's business; (b) the type of information that LangChain will store; and (c) the need for security and confidentiality of such information.

LangChain's security program includes:

1. **Security Awareness and Training**. A mandatory security awareness and training program for all members of LangChain's workforce (including management), which includes:

- Training on how to implement and comply with its Information Security Program; and
- Promoting a culture of security awareness through periodic communications from senior management with employees.

2. **Access Controls**. Policies, procedures, and logical controls:

- To limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons;
- To prevent those workforce members and others who should not have access from obtaining access; and
- To remove access in a timely basis in the event of a change in job responsibilities or job status.

3. **Security Incident Procedures**. A security incident response plan that includes procedures to be followed in the event of any Security Breach. Such procedures include:

- Roles and responsibilities: formation of an internal incident response team with a response leader;
- Investigation: assessing the risk the incident poses and determining who may be affected;
- Communication: internal reporting as well as a notification process in the event of unauthorized disclosure of Customer Data;
- Recordkeeping: keeping a record of what was done and by whom to help in later analysis and possible legal action; and
- Audit: conducting and documenting root cause analysis and remediation plan.

4. **Contingency Planning**. Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, pandemic flu, and natural disaster) that could damage Customer Data or production systems that contain Customer Data. Such procedures include:

- Data Backups: A policy for performing periodic backups of production data sources, as applicable, according to a defined schedule;
- Disaster Recovery: A formal disaster recovery plan for the production data center, including:
  - Requirements for the disaster plan to be tested on a regular basis, currently twice a year; and
  - A documented executive summary of the Disaster Recovery testing, at least annually, which is available upon request to customers.

- Business Continuity Plan: A formal process to address the framework by which an unplanned event might be managed in order to minimize the loss of vital resources.

5. **Audit Controls**. Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information.

6. **Data Integrity**. Policies and procedures to ensure the confidentiality, integrity, and availability of Customer Data and protect it from disclosure, improper alteration, or destruction.

7. **Storage and Transmission Security**. Security measures to guard against unauthorized access to Customer Data that is being transmitted over a public electronic communications network or stored electronically. Such measures include requiring encryption of any Customer Data stored on desktops, laptops or other removable storage devices.

8. **Secure Disposal**. Policies and procedures regarding the secure disposal of tangible property containing Customer Data, taking into account available technology so that Customer Data cannot be practicably read or reconstructed.

9. **Assigned Security Responsibility**. Assigning responsibility for the development, implementation, and maintenance of LangChain's security program, including:

- Designating a security official with overall responsibility;
- Defining security roles and responsibilities for individuals with security responsibilities; and
- Designating a Security Council consisting of cross-functional management representatives to meet on a regular basis.

10. **Monitoring**. Network and systems monitoring, including error logs on servers, disks and security events for any potential problems. Such monitoring includes:

- Reviewing changes affecting systems handling authentication, authorization, and auditing;
- Reviewing privileged access to LangChain production systems; and
- Engaging third parties to perform network vulnerability assessments.

11. **Change and Configuration Management**. Maintaining policies and procedures for managing changes LangChain makes to production systems, applications, and databases. Such policies and procedures include:

- process for documenting, testing and approving the patching and maintenance of the LangChain's software;
- A security patching process that requires patching systems in a timely manner based on a risk analysis; and
- A process for LangChain to utilize a third party to conduct application level security assessments. These assessments generally include testing, where applicable, for:
    - Cross-site request forgery
    - Services scanning

- Improper input handling (e.g. cross-site scripting, SQL injection, XML injection, cross-site flashing)
- XML and SOAP attacks
- Weak session management
- Data validation flaws and data model constraint inconsistencies
- Insufficient authentication
- Insufficient authorization

12. **Program Adjustments**. Monitoring, evaluating, and adjusting, as appropriate, the security program in light of:

- Any relevant changes in technology and any internal or external threats to LangChain or the Customer Data;
- Security and data privacy regulations applicable to LangChain; and
- LangChain's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

13. **Devices** – Ensuring that all laptop and desktop computing devices utilized by LangChain and its employees when accessing Customer Data:

- will be equipped with a minimum of AES 128 bit full hard disk drive encryption;
- will have up to date virus and malware detection and prevention software installed with virus definitions updated on a regular basis; and
- will maintain virus and malware detection and prevention software so as to remain on a supported release. This will include, but not be limited to, promptly implementing any applicable security-related enhancement or fix made available by the supplier of such software.