Privacy, Confidentiality, and Data Protection Agreement

1. Purpose

This Privacy, Confidentiality, and Data Protection Agreement ("Agreement") governs the collection, access, processing, storage, transmission, and deletion of Client Data by the Service Provider in connection with the technology consulting, advisory, implementation, support, and related professional services provided to the Client.

2. Definitions

"Client" means the entity receiving services from the Service Provider.

"Service Provider" means INDIVIDUAL CONTRIBUTOR LLC, including its employees, contractors, affiliates, and authorized representatives engaged in performing the Services.

"Client Data" means any information, data, records, documents, databases, files, systems, credentials, configurations, intellectual property, or other materials provided by, made available by, or accessed on behalf of the Client during the performance of the Services.

"Services" means the technology consulting, implementation, development, support, advisory, and related services performed by the Service Provider pursuant to the applicable agreement between the parties.

3. Data Access and Processing

3.1 The Service Provider shall access, use, and process Client Data solely for the purpose of performing the Services and fulfilling its contractual obligations.

3.2 The Service Provider shall not sell, disclose, transfer, distribute, commercialize, or otherwise use Client Data for any purpose unrelated to the Services without the Client's prior written consent.

3.3 Access to Client Data shall be limited to personnel who have a legitimate business need to access such information for the performance of the Services.

need to access such information for the performance of the Services.

3.4 The Service Provider shall implement and maintain the principle of least privilege, ensuring that personnel are granted only the minimum level of access necessary to perform their assigned responsibilities.

4. Information Security Measures

4.1 The Service Provider shall maintain reasonable and appropriate administrative, technical, and organizational safeguards designed to protect Client Data against unauthorized access, disclosure, alteration, loss, destruction, or misuse.

4.2 Such safeguards may include, as applicable:

a. Role-based access controls;

b. Authentication and authorization mechanisms;

c. Encryption of data in transit and, where applicable, at rest;

d. Secure network and endpoint protection measures;

e. Access logging and monitoring;

f. Personnel confidentiality obligations; and

g. Security awareness and operational procedures.

4.3 The Service Provider shall periodically review access rights and promptly revoke access that is no longer required for service delivery.

5. Temporary Storage and Data Retention

5.1 The Service Provider may temporarily store or cache Client Data only to the extent reasonably necessary for the provision, maintenance, troubleshooting, testing, or support of the Services.

5.2 The Service Provider shall not retain Client Data longer than necessary to fulfill the purposes for which such data was accessed or processed.

5.3 Any temporary local copies, backups, logs, extracts, datasets, or other forms of Client Data maintained by the Service Provider shall be protected in accordance with this Agreement.

Agreement.

6. Confidentiality

6.1 All Client Data shall be deemed Confidential Information of the Client.

6.2 The Service Provider shall maintain the confidentiality of Client Data and shall not disclose such information to any third party except:

a. As required to perform the Services;

b. With the Client's prior written authorization; or

c. As required by applicable law, regulation, court order, or governmental authority.

6.3 In the event disclosure is legally required, the Service Provider shall, to the extent legally permissible, provide prompt notice to the Client to allow the Client an opportunity to seek protective measures.

7. Subcontractors and Personnel

7.1 The Service Provider shall ensure that its employees, contractors, agents, and subcontractors who may access Client Data are bound by confidentiality and data protection obligations no less protective than those contained in this Agreement.

7.2 The Service Provider shall remain responsible for the acts and omissions of its personnel and approved subcontractors relating to Client Data.

8. Data Breach Notification

8.1 The Service Provider shall promptly notify the Client upon becoming aware of any confirmed unauthorized access to, disclosure of, or loss of Client Data that materially affects the confidentiality, integrity, or availability of such data.

8.2 The notification shall include, to the extent reasonably available:

a. A description of the nature of the incident;

b. The categories of affected data;

c. The remediation measures undertaken; and

d. Recommended actions, if any, for the Client.

d. Recommended actions, if any, for the Client.

8.3 The Service Provider shall cooperate in good faith with the Client in investigating and mitigating the effects of any such incident.

9. Return and Deletion of Data Upon Termination

9.1 Upon expiration or termination of the applicable services agreement, or upon the Client's written request, the Service Provider shall promptly cease accessing Client Data except as otherwise required by law.

9.2 Within thirty (30) days following termination of the Services, or such other period agreed by the parties in writing, the Service Provider shall:

a. Return any Client Data requested by the Client; and/or

b. Permanently delete or securely destroy all Client Data in its possession, custody, or control, including any temporary local copies, caches, extracts, backups, or derivative datasets, except where retention is required by applicable law.

9.3 Upon written request, the Service Provider shall provide a written certification confirming the completion of the deletion or destruction process.

9.4 Any retained data required by law shall remain subject to the confidentiality and security obligations set forth in this Agreement until such data is lawfully deleted.

10. Compliance with Applicable Laws

Each party shall comply with all applicable privacy, data protection, cybersecurity, and information security laws and regulations relevant to its obligations under this Agreement.

11. Survival

The obligations relating to confidentiality, data protection, data deletion, and restrictions on the use of Client Data shall survive the termination or expiration of the Services for so long as the Service Provider possesses or is legally required to retain Client Data.

12. Order of Precedence

In the event of any conflict between this Agreement and any other agreement governing the Services, the provision affording the greater level of protection to Client Data shall prevail, unless otherwise expressly agreed in writing by the parties.

prevail, unless otherwise expressly agreed in writing by the parties.