DATA PROTECTION AND SECURITY AGREEMENT
FOR AUDIT AND ASSURANCE SERVICES

This Data Protection and Security Agreement (the "Agreement") is entered into and made effective as of _____, 20_____ (the "Effective Date"), by and between:

Client: _____
Address: _____
Represented by: _____

And

Assurance Provider: _____
Address: _____
Represented by: _____

Each of the parties above may be referred to individually as a "Party" and collectively as the "Parties."

1. PURPOSE AND SCOPE

1.1. The Assurance Provider has been engaged to perform certain audit and assurance services (the "Services") for the Client pursuant to the engagement letter dated _____.

1.2. In the course of performing the Services, the Assurance Provider may receive, access, maintain, process, or transmit sensitive financial, proprietary, and personal data (collectively, "Assurance Data").

1.3. This Agreement sets forth the technical, organizational, and security measures the Assurance Provider must implement and maintain to safeguard Assurance Data against unauthorized access, disclosure, alteration, or destruction.

2. DEFINITIONS

2.1. **"Assurance Data"** means any information, including personal data, financial records, proprietary corporate information, and audit evidence, provided by or on behalf of the Client to the Assurance Provider for the purpose of executing the Services.

2.2. **"Data Protection Laws"** means all applicable regional, national, and international laws, rules, regulations, and directives governing privacy, data security, and the processing of personal information.

2.3. **"Security Incident"** means any suspected or confirmed unauthorized access, acquisition, disclosure, alteration, loss, or destruction of Assurance Data.

3. DATA HANDLING AND CONFIDENTIALITY

3.1. **Purpose Limitation:** The Assurance Provider shall process Assurance Data solely for the purpose of providing the Services and in accordance with the documented instructions of the Client.

3.2. **Confidentiality:** The Assurance Provider shall ensure that all personnel authorized to process Assurance Data are bound by strict obligations of confidentiality.

3.3. **Data Minimization:** The Assurance Provider shall restrict access to Assurance Data to those employees, contractors, and subcontractors who require access to fulfill the specific objectives of the Services.

4. TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

4.1. The Assurance Provider shall implement and maintain appropriate administrative, physical, and technical safeguards to protect the security, integrity, and confidentiality of Assurance Data, including but not limited to:

- Encryption of Assurance Data both in transit and at rest.
- Multi-factor authentication (MFA) for all access to systems containing Assurance Data.
- Regular vulnerability scanning, penetration testing, and risk assessments.
- Physical access controls for all facilities housing hardware that stores or processes Assurance Data.
- Restricting data transfers to authorized environments and devices only.

5. SECURITY INCIDENT RESPONSE AND NOTIFICATION

5.1. **Notification:** The Assurance Provider shall notify the Client in writing without undue delay, and in any event within _____ hours, after becoming aware of any Security Incident.

5.2. **Content of Notification:** The notification shall, at a minimum, describe the nature of the Security Incident, the categories and approximate number of records affected, and the mitigation measures taken or planned.

5.3. **Mitigation:** The Assurance Provider shall immediately take all necessary steps to mitigate the impact of the Security Incident and preserve forensic evidence.

6. AUDIT AND COMPLIANCE RIGHTS

6.1. **Right to Audit:** No more than once per calendar year, unless a Security Incident has occurred, the Client or its designated independent auditor shall have the right to audit the Assurance Provider's compliance with this Agreement.

6.2. **Cooperation:** The Assurance Provider shall cooperate fully with such audits and provide access to relevant security policies, system logs, certification reports (e.g., SOC 2, ISO 27001), and personnel.

7. SUBPROCESSORS

7.1. The Assurance Provider shall not engage any third-party subprocessor to access or process Assurance Data without prior written authorization from the Client.

7.2. If authorized, the Assurance Provider shall impose written data protection obligations on the subprocessor that are no less restrictive than those set forth in this Agreement.

8. TERM AND TERMINATION

8.1. **Term:** This Agreement shall commence on the Effective Date and remain in effect until the termination of the primary services agreement or until all Assurance Data has been deleted or returned.

8.2. **Data Return or Destruction:** Within _____ days of termination of the Services, the Assurance Provider shall, at the option of the Client, securely return or permanently delete all copies of Assurance Data, unless applicable laws or professional standards require retention.

IN WITNESS WHEREOF, the Parties have executed this Data Protection and Security Agreement as of the Effective Date.

FOR CLIENT:

Signature: _____

Name: _____

Title: _____

Date: _____

FOR ASSURANCE PROVIDER:

Signature: _____

Name: _____

Title: _____

Date: _____