INFORMATION SECURITY AGREEMENT

for Audit and Assurance Services

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

Client: _____, with its principal place of business at _____

And

Auditor: _____, with its principal place of business at _____

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

1. PURPOSE

The Auditor has been engaged to perform certain audit and assurance services for the Client pursuant to an engagement letter or master services agreement dated _____ (the "Main Agreement"). In connection with these services, the Client will disclose to the Auditor certain highly sensitive, confidential, and proprietary financial, operational, and personal data. This Agreement defines the information security requirements and data protection obligations the Auditor must maintain to safeguard this data.

2. DEFINITION OF AUDIT DATA

"Audit Data" refers to any and all information, data, documents, records, or credentials provided by or on behalf of the Client to the Auditor for the performance of the audit services, whether in oral, visual, electronic, or written form, containing but not limited to financial records, trade secrets, personally identifiable information (PII), system configurations, intellectual property, and proprietary internal controls.

3. CONFIDENTIALITY AND ACCESS CONTROL

1. The Auditor shall restrict access to Audit Data solely to those employees, agents, and authorized subcontractors who have a legitimate "need-to-know" for the performance of the audit.
2. The Auditor shall ensure that all personnel with access to Audit Data are bound by written confidentiality obligations no less restrictive than those contained herein.
3. The Auditor shall implement role-based access controls, ensuring that access to the Client's system environments and data repositories is limited to authorized personnel only.

4. TECHNICAL AND ORGANIZATIONAL SAFEGUARDS

1. **Data Encryption:** The Auditor shall encrypt all Audit Data both in transit using secure protocols (e.g., TLS 1.2 or higher) and at rest using industry-standard encryption algorithms (e.g., AES-256).
2. **Storage and Transmission:** Audit Data must only be stored on secure, managed systems owned or controlled by the Auditor. Transmission of Audit Data via unencrypted channels, such as standard email, is strictly prohibited.
3. **Multi-Factor Authentication (MFA):** The Auditor shall enforce MFA for all user accounts and remote connections accessing systems containing Audit Data.
4. **Vulnerability and Patch Management:** The Auditor shall maintain an active patch management policy to ensure that all

operating systems, applications, and network infrastructure handling Audit Data are updated against known vulnerabilities.

5. SECURITY INCIDENT AND BREACH NOTIFICATION

1. The Auditor shall maintain a documented incident response plan.
2. In the event of any suspected or confirmed unauthorized access, acquisition, alteration, loss, or disclosure of Audit Data (a "Security Incident"), the Auditor shall notify the Client in writing within _____ hours of discovery.
3. The notification shall include, at minimum, a description of the nature of the incident, the categories of data affected, and the corrective actions being taken.
4. The Auditor shall, at its own expense, cooperate fully with the Client's investigation, forensic analysis, and mitigation efforts related to the Security Incident.

6. DATA RETENTION AND DESTRUCTION

1. Upon the conclusion of the audit services or upon the written request of the Client, the Auditor shall securely delete, destroy, or return all copies of the Audit Data, except to the extent that professional standards or regulatory retention periods require the preservation of working papers.
2. Any retained Audit Data shall continue to be protected in accordance with this Agreement for as long as it remains in the possession or control of the Auditor.
3. The Auditor shall utilize secure destruction methods (such as cryptographic erasure or physical degaussing) that render the data completely unrecoverable.

7. COMPLIANCE AND AUDITING RIGHTS

1. The Auditor represents and warrants that its security program aligns with recognized industry frameworks (e.g., SOC 2 Type II, ISO/IEC 27001).
2. Upon reasonable prior notice, the Client shall have the right to review the Auditor's security policies, standard operating procedures, and third-party security certifications or audit summaries.

8. TERM AND TERMINATION

This Agreement shall remain in effect for the duration of the Main Agreement and shall survive the termination of the Main Agreement for as long as the Auditor retains any portion of the Audit Data.

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

For the Client:	**For the Auditor:**
_____	_____
Authorized Signature	Authorized Signature
_____	_____
Printed Name	Printed Name
_____	_____
Title	Title
_____	_____
Date	Date