# FINANCIAL AUDIT INFORMATION SECURITY AGREEMENT

*Audit and Assurance Services*

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

**Auditee / Client:** _____

Address: _____

**Auditor / Assurance Provider:** _____

Address: _____

## 1. PURPOSE

The purpose of this Agreement is to establish the information security requirements, obligations, and protocols to protect the confidentiality, integrity, and availability of all financial and proprietary information provided to the Auditor in connection with the financial audit and assurance services for the fiscal period _____ to _____.

## 2. DEFINITION OF AUDIT DATA

"Audit Data" refers to any and all financial records, transaction logs, bank statements, tax documents, employee payroll records, system configurations, proprietary business processes, and personal data disclosed by the Auditee to the Auditor, whether orally, in writing, or in electronic format.

## 3. CONFIDENTIALITY AND ACCESS CONTROL

1. The Auditor shall restrict access to the Audit Data solely to authorized personnel who have a direct professional need to know in connection with the audit services.
2. The Auditor shall ensure that all personnel assigned to the audit have undergone background checks and are bound by professional confidentiality obligations.
3. No Audit Data shall be shared with, disclosed to, or accessed by any third party without prior written consent from the Auditee, except as required by applicable professional standards or statutory regulations.

## 4. DATA SECURITY PROTOCOLS

1. **Transmission Security:** All electronic Audit Data transmitted between the parties shall be encrypted in transit using industry-standard protocols.
2. **Storage Security:** The Auditor shall store all digital and physical Audit Data in secure environments with restricted physical and logical access control mechanisms.
3. **Device Security:** Any device used by the Auditor to access or process Audit Data must be equipped with active firewalls, up-to-date antivirus software, and full-disk encryption.

## 5. SECURITY INCIDENT AND BREACH NOTIFICATION

1. The Auditor shall maintain active monitoring systems to detect unauthorized access, exposure, or modification of the Audit Data.
2. In the event of a suspected or confirmed data security breach involving Audit Data, the Auditor must notify the Auditee in writing within _____ hours of discovery.
3. The Auditor shall fully cooperate with the Auditee to investigate, mitigate, and remediate any such security incident.

## 6. DATA RETENTION AND DESTRUCTION

1. Upon the completion of the audit services and the issuance of the final audit report, the Auditor shall retain the required audit documentation only for the minimum period mandated by professional standards and statutory retention requirements.
2. Except for required retention documentation, all other copies of Audit Data, whether digital or physical, must be securely deleted or destroyed within _____ days of the conclusion of the engagement. Physical records must be shredded, and digital files must be securely wiped.

## 7. TERM AND GOVERNING LAW

This Agreement shall remain in effect throughout the duration of the audit engagement and shall survive the termination of the professional relationship. This Agreement shall be governed by and construed in accordance with the laws of _____.

IN WITNESS WHEREOF, the parties hereto have executed this Financial Audit Information Security Agreement as of the Effective Date.

| **FOR THE AUDITEE:** | **FOR THE AUDITOR:** |
| --- | --- |
| _____ | _____ |
| **Authorized Signature** | **Authorized Signature** |
| _____ | _____ |
| **Printed Name** | **Printed Name** |
| _____ | _____ |
| **Title** | **Title** |
| _____ | _____ |
| **Date** | **Date** |