

WRITTEN INFORMATION SECURITY PLAN (WISP)

Firm Name: Shubham Kothari & Associates, Chartered Accountants, India

Effective Date: April 1, 2026

Designated Security Coordinator: CA Shubham Kothari

1. PURPOSE & SCOPE

This Written Information Security Plan ("WISP") outlines the administrative, technical and physical safeguards the Firm uses to protect confidential client information in its Global Accounting practice. It applies to all team members working on Global Accounting engagements.

2. DATA ENCRYPTION & TRANSMISSION STANDARDS

- **In-Transit Protection:** Sensitive client files are shared only through encrypted email or secure folders.
- **Secure Storage:** Client documents are kept within the Firm's secure cloud environment.
- **Secure File Sharing:** File transfers with clients take place through restricted, invite-only folders, with access permissions managed by the Designated Security Coordinator.

3. ACCESS CONTROLS

- **Multi-Factor Authentication (MFA):** Two-step verification is used for firm email, cloud storage and client accounting platforms (such as QuickBooks Online), wherever the platform supports it.
- **Passwords:** Strong passwords are used for firm devices and systems.
- **Session Locks:** Workstations lock automatically after a period of inactivity.
- **Restricted Access:** Access to client information is limited to the team members working on that client's engagement.

4. LOCAL STORAGE POLICY

- **Cloud-Based Work:** Client financial records and source documents are kept off the hard drives of local workstations.
- **Remote Processing:** Bookkeeping and cleanup work is performed within the client's cloud accounting environment or through secure remote access provided by the client.
- **Temporary Files:** Any temporary files or downloads are deleted at the end of the working session.

5. PHYSICAL SECURITY & ACCESS

- **Workstation Security:** Office workstations are kept in an area accessible only to authorised personnel.
- **Clean Desk:** Physical documents containing client information are kept secured when unattended.
- **Secure Destruction:** Physical copies of client information are shredded once the task is complete.

6. OVERSIGHT & INCIDENT RESPONSE

- **Oversight:** The Designated Security Coordinator periodically reviews these safeguards.
- **Incident Response:** If a security incident is suspected, the Designated Security Coordinator will end active sessions, secure affected access and notify the affected clients promptly.

Shubham Kothari & Associates

Chartered Accountants

CA Shubham Kothari

Proprietor