DATA SECURITY POLICY

We are an ISO 9001:2008 and ISO 27001 certified organisation and have strict policies and processes to ensure that client data remains secure and confidential. Whether it is corporate management, financial management, HR management, or risk management, confidentiality is an integral part of our program. We ensure confidentiality through controlled access and strict data retention policies.

SECURITY MEASURES:

- **Controlled Access:** All our employees are in-house and work on designated computers with appropriate restrictions on data sharing and storage.
- **Restricted Access to Websites:** We restrict access to websites, limiting use to only those required for service requirements.
- **Physical Security Measures:** Systems are disabled for external storage devices (e.g., pen drives, CD-ROMs) except for company emails and internet servers.

NON-DISCLOSURE AGREEMENTS:

- We enter into non-disclosure and confidentiality agreements with our clients to ensure their data remains protected.
- Employees are legally bound by contract to maintain the confidentiality of all client and company data, prohibiting them from stealing, sharing, or copying any data for unauthorized use.

HANDLING CONFIDENTIAL DATA:

- **Secure FTP Portal:** Data is shared via a private, encrypted link where you maintain full authority to upload or delete files. Access is strictly limited to authorized users to ensure your data remains private and protected.
- **Validation:** We implement automated validation checks at data entry points to ensure that only accurate and complete information is processed. This includes real-time checks for format consistency, range constraints, and cross-field validation to prevent errors and ensure uncorrupted data transmission.
- **Storage:** All data is stored on network servers with a best-in-class storage system, featuring remote back-up, security, and firewall protection.
- **BCP:** A copy of data is stored in an alternate location for secure backup.
- **Retention:** Confidential data is stored for up to three months after the termination of the business relationship, unless specifically requested by the client to retain the data for a longer period.

NON-PUBLIC PERSONAL INFORMATION:

All data collected from our clients through interviews, written communication, emails, and prior tax returns is never disclosed except as required by law.

©Mercurius Advisory Services