Client Data Confidentiality Policy

Status Completed

Date Created Sep 1, 2025

Date Updated Sep 9, 2025

Owner Tony Adams

Introduction

At Spottletoe Project Consulting [“Spottletoe”], we understand that the information you share with us is sensitive and critical to your business. Your trust is our most important asset. This Confidentiality Policy outlines our firm commitment to protecting your data and describes the specific measures we take to ensure its security and privacy.

Definition of Confidential Information

For the purposes of our engagement, "Confidential Information" includes, but is not limited to:

- Business strategies, financial data, and forecasts
- Customer lists, supplier details, and partner information
- Operational processes, trade secrets, and intellectual property
- Marketing plans, sales data, and performance metrics
- Any other non-public information you disclose to us for the purpose of our consultancy services

How We Handle Your Information

Our handling of your data is governed by three core principles:

1. **Need-to-Know Access**: Your confidential information is accessible only to [the specific consultants] directly working on your project. We do not share your data with any third parties without your explicit prior consent, unless required by law (see Section 6).
2. **Exclusive Use**: Your data will be used solely for the purpose of delivering the consultancy services we have been engaged for. It will never be used for any other purpose or for the benefit of any other client.
3. **Minimum Necessary**: We will only collect and retain the information that is absolutely necessary to achieve the objectives of our engagement.

Our Data Protection Measures

We employ a multi-layered approach to safeguard your information, combining physical, technical, and administrative security measures.

Digital Security

Encryption: At Spottletoe, we use Google Workspace to manage and store our data. Our data stored on Google Workspace is encrypted at rest using industry-standard encryption (AES-256), while data transmitted electronically (e.g., via email or file transfer) is protected using TLS/SSL encryption.

Secure Storage: Client files are stored on password-protected, encrypted cloud services with robust security practices (Google Workspace).

Device Security: All devices (laptops, phones, tablets) used to access your data are secured with strong passcodes/passwords, disk encryption, and up-to-date antivirus software.

Secure Communication: We use secure methods for sharing sensitive files, such as encrypted email, password-protected files (with the password sent separately), or secure client portals.

Administrative & Physical Security

Confidentiality Agreements: All Spottletoe employees or consultants working with clients are bound by strict confidentiality agreements that extend to client information.

Physical Measures: Any physical documents are stored in a locked cabinet when not in use and are securely shredded at the end of our engagement or when no longer needed.

Clean Desk Policy: We maintain a clean desk policy to ensure that confidential information is not left unattended.

Data Retention & Disposal

We will retain your confidential information only for as long as necessary to fulfill the purposes outlined in our engagement agreement, or as required by law. Upon termination of our engagement or at your request, we will promptly:

- Securely delete or destroy all electronic copies of your data from our active systems and backups according to a secure deletion schedule.
- Securely shred any physical documents containing your confidential information.

You may request the return of your data at any time during the engagement.

Limitations

Our confidentiality obligations shall not apply to information that:

- Was already lawfully in our possession before you disclosed it.
- Is or becomes publicly available through no fault of our own.
- Is lawfully disclosed to us by a third party without restriction.

- We are required to disclose by law, court order, or governmental authority. In such a case, unless legally prohibited, we will notify you promptly to allow you to seek a protective order.

Our Commitment

Data security is an ongoing process. We are committed to regularly reviewing and updating our security practices and this policy to adapt to new technologies and evolving threats.

Contact Us

If you have any questions about this Confidentiality Policy or how your data is handled, please do not hesitate to contact us at support@spottletoe.com