Internal Data & Security Policy

1. Purpose & Scope

This internal operational document establishes baseline cybersecurity and data management protocols for JTL Events Management Ltd (trading as JTL Events). As a sole operator utilizing cloud tools, website software, and HubSpot CRM, maintaining strict cyber hygiene protects operational continuity, client data, and business liability.

2. Access Controls & Password Management

- **Password Policy:** All critical business platforms (Hubspot CRM, Website Backend, Email, Accounting) must utilize unique, complex passwords.
- **Password Manager:** Master credentials must be stored securely using a dedicated password manager (e.g., 1Password or Bitwarden).
- **Multi-Factor Authentication (2FA):** 2FA must be strictly enabled across all primary service accounts, specifically the CRM, website management platform, domain registrar, and financial applications.

3. HubSpot CRM Management & Data Hygiene

- **HubSpot User Access:** Access to the HubSpot CRM account is restricted exclusively to the primary operator. Any future contractor access must adhere to the principle of least privilege.
- **Data Minimization:** Do not collect unnecessary personal information in HubSpot. Remove sensitive, event-specific details (e.g., special dietary or accessibility notes) once the event has concluded.
- **Routine Audits:** Conduct annual reviews of the HubSpot CRM database to purge unengaged contacts, soft bounces, and duplicate records.
- **API & Integration Security:** Review connected HubSpot integrations, plugins, and third-party apps annually to revoke unused access permissions.

4. Backup & Recovery Protocols

- **Website Backups:** Automated daily or weekly cloud backups must be configured for the website database and file assets.

- **HubSpot CRM Data Export:** Generate quarterly offline CSV exports of primary contact lists, customer lists, and financial transaction history from HubSpot to store in an encrypted backup location.
- **Device Backups:** Business hardware (laptops, phones) must utilize automated encrypted cloud backup systems.

5. Device Security

- **Device Lock:** All work devices (laptop, mobile) must require biometric authentication or a PIN/passcode when idle.
- **Software Updates:** Operating systems, antivirus software, and web applications/plugins must be kept updated to patch security vulnerabilities.

6. Document Control & Review Schedule

Parameter	Details
Document Title	Internal Data and Security Policy
Owner / Responsible Person	Janine Tompkins, Director
Current Version	Version 1.0
Date Last Reviewed	28 July 2026
Next Scheduled Review	28 July 2027