Mac Smart
Privacy & Data Handling Policy

1. Scope

This policy covers how Mac Technical Support Pty Ltd (Mac Smart) collects, uses, and protects personal and technical information belonging to its clients and website visitors.

2. Information Collection

- **Direct Collection:** We collect names, emails, and phone numbers via our website contact form for the purpose of responding to service inquiries.
- **Service Delivery Data:** To provide managed IT services, we store technical data including network configurations, device identifiers, and administrative credentials.
- **Credential Management:** Client passwords and sensitive access keys are managed using hardware-encrypted vaults (Apple Keychain) and MFA-protected, restricted-access documentation within Google Workspace.

3. Use of Data

Data is used solely for the purpose of:

- Providing technical support and network management.
- Monitoring system health and security (via SentinelOne/UniFi).
- Performing offsite backups as per service agreements.

4. Data Security & Storage

- **Encryption:** All data "at rest" on Mac Smart systems is encrypted using FileVault or equivalent hardware encryption.
- **Access Control:** Multi-Factor Authentication (MFA) is mandatory for all administrative portals, including Google Workspace and Network management tools.
- **Backups:** Our standard professional recommendation and service model is based on a 3-2-1 backup methodology. Where engaged to do so, we facilitate the storage of client data across multiple locations, including encrypted offsite cloud repositories and local hardware-encrypted storage. The specific backup configuration for each client is determined by their individual service agreement and infrastructure requirements.

5. Data Retention & Destruction

- **Financial Records:** Retained for 7 years as per Australian tax law.
- **Client Technical Data:** Retained for the duration of the service agreement.
- **Destruction:** Upon termination of services, client credentials are removed from our repositories within 30 days. Physical media (hard drives) are cryptographically wiped or physically destroyed before disposal.

6. Disclosure to Third Parties

We do not sell client data. Technical data may be shared with upstream vendors (e.g., Apple, Google, Ubiquiti) only as required for hardware warranty or cloud service provisioning.