SoulShine AI Public Security & Compliance Statement

Entity: Soul Kitchen AI Inc., d/b/a SoulShine AI

1. Our Commitment to Ministry Security

At SoulShine AI, we understand that trust is the currency of ministry. We employ a multi-layered, enterprise-grade security architecture designed to safeguard your congregation's data and ensure platform integrity. This document outlines our technical safeguards and the shared operational responsibilities required to maintain a secure digital environment.

2. Technical Infrastructure & Data Governance

We operate a strict "Walled Garden" approach to your data, fortified by the following technical measures:

- **End-to-End Encryption:** All user data is secured using robust encryption algorithms both in transit and at rest, rendering it unreadable to unauthorized parties.

- **Strict Access Control:** We enforce role-based access control (RBAC), ensuring only authorized personnel with a legitimate, documented need can access critical systems.

- **Data Minimization:** To inherently reduce risk, the platform is engineered to collect only the minimum necessary user data required to execute its services.

- **Continuous Threat Monitoring:** We utilize real-time intrusion detection systems to monitor network traffic for suspicious activity, alongside routine vulnerability scanning and penetration testing to proactively identify potential weaknesses.

- **Secure Cloud Infrastructure & Disaster Recovery:** The platform is hosted on secure, resilient cloud infrastructure featuring redundant systems, strict firewalls, and regular offsite data backups to ensure rapid disaster recovery and business continuity.

3. The Shared Responsibility Model

Security is an ongoing, collaborative process. While SoulShine AI secures the underlying infrastructure, the Customer (the Ministry) retains critical responsibilities regarding account access and usage:

- **Credential Management:** Users must utilize strong, unique passwords and are strongly encouraged to enable multi-factor authentication (MFA) to prevent account takeover.

- **Endpoint Security:** The Customer is responsible for ensuring that all devices used to access the platform are secure, up-to-date with security software, and protected against malware.

- **Internal Access Audits:** Ministry administrators are responsible for conducting periodic reviews of their internal access control lists to ensure only current, authorized staff retain platform access.

4. Legal Disclaimers & Limitation of Liability

- **"As-Is" Provision:** While SoulShine AI implements rigorous security measures, the platform and its related services are provided on an "as-is" and "as-available" basis. We cannot guarantee that the platform will be entirely immune to all unauthorized access or zero-day vulnerabilities.

- **Limitation of Liability:** To the maximum extent permitted by applicable law, Soul Kitchen AI Inc., including its founders, directors, and officers, shall not be held liable for any direct, indirect, incidental, consequential, or special damages arising out of a data breach, cyber-attack, or unauthorized access event, provided the Company has not acted with gross negligence.

- **Customer Indemnification:** The Company assumes no liability for security breaches resulting directly from the Customer's failure to adhere to the Shared Responsibility Model (e.g., falling victim to phishing attacks, sharing credentials, or utilizing compromised devices).