

SoulShine AI: Trust and Security Brief

1. Our Philosophy: The "Walled Garden"

At SoulShine AI, we recognize that trust is the currency of ministry. We have engineered a multi-layered security architecture designed to safeguard your congregation's sensitive data while ensuring absolute platform integrity. We treat your information as a sacred asset, protected by enterprise-grade infrastructure.

2. Technical Infrastructure & Data Governance

We employ industry best practices to ensure your ministry's data remains confidential and available exclusively to authorized users.

- **Military-Grade Encryption:** All user data is encrypted using robust algorithms both in transit and at rest, rendering it entirely unreadable if intercepted.
- **Strict Access Control (RBAC):** We enforce role-based access control, ensuring that only personnel with a legitimate, documented need can access critical systems.
- **Data Minimization:** Our platform is engineered to collect only the absolute minimum data required to execute its services, inherently reducing the impact of any potential exposure.
- **Resilient Infrastructure & Recovery:** The platform is hosted on secure cloud infrastructure featuring redundant systems, strict firewalls, and regular offsite data backups to guarantee rapid disaster recovery.

3. Proactive Threat Defense

We do not wait for threats; we actively hunt them.

- **Continuous Monitoring:** We utilize real-time intrusion detection systems to monitor network traffic for suspicious activity.
- **Routine Vulnerability Scanning:** We conduct regular penetration testing and vulnerability scans to proactively identify and neutralize potential weaknesses.
- **Secure Development:** Security is built into our software development lifecycle, utilizing code reviews, static analysis, and dynamic testing.

4. The Shared Responsibility Model

Security is a collaborative operational requirement. While SoulShine AI secures the underlying infrastructure, the Customer (the Ministry) retains critical responsibilities regarding platform access:

- **Credential Management:** Users must utilize strong, unique passwords and are strongly encouraged to enable multi-factor authentication (MFA) to prevent account takeover.
- **Endpoint & Phishing Security:** The Customer is responsible for ensuring their accessing devices are protected against malware and that staff are trained to recognize phishing attempts.
- **Administrative Access Audits:** Ministry administrators must conduct periodic reviews of internal access control lists to ensure only current, authorized staff retain platform access.

5. Legal Safeguards & Limitation of Liability

- **"As-Is" Provision:** While SoulShine AI implements rigorous, state-of-the-art 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.
- **Customer Indemnification:** The Company assumes no liability for security breaches resulting directly from the Customer's failure to adhere to the Shared Responsibility Model, including compromised credentials or unsecure endpoint devices.