PRIVACY POLICY & DATA SOVEREIGNTY STATEMENT

Last Updated: March 4, 2026

1. OPERATIONAL DOCTRINE Concierge Defense ("The Firm," "We," "Us") operates as a retained crisis authority. We adhere to a doctrine of **Data Minimalism**. We do not monetize user data. We do not operate advertising trackers. We exist to protect the sovereignty of our Principals, not to harvest their digital exhaust.

This Privacy Policy governs the collection, use, and defense of information obtained through `conciergedefense.com` (the "Site") and preliminary operational inquiries.

CRITICAL DISTINCTION: This policy applies to *public site visitors and initial inquiries*. Data collected during active client engagements (e.g., threat intelligence, biometric data, asset ledgers) is governed exclusively by the **Master Services Agreement (MSA)** and executing **Non-Disclosure Agreements (NDAs)**, which supersede this document.

2. COLLECTION OF INTELLIGENCE (DATA TYPES) We limit collection to the absolute minimum required to establish a secure channel of communication or verify a referral.

A. Voluntarily Provided Information We may collect the following when you initiate a secure inquiry or referral verification:

- **Cryptographic Keys:** PGP Public Keys or similar identifiers for secure channel establishment.
- **Contact Coordinates:** Business email addresses (we advise against using personal email for initial contact).
- **Referral Tokens:** Unique identifiers provided by existing Principals to verify your eligibility for intake.

B. Automated Technical Telemetry (Site Defense) To protect our infrastructure from hostile reconnaissance, we automatically collect specific technical data. This is used solely for defensive counter-intelligence and site integrity:

- **IP Addresses & Geolocation:** Logged for threat analysis and geo-blocking of hostile jurisdictions.
- **User Agent & Device Fingerprints:** Used to identify botnets or automated scraping tools.
- **Access Timestamps:** Retained for forensic audit trails in the event of a security incident.

3. USE OF INFORMATION We use your data for three specific purposes:

1. **Verification:** To authenticate your identity and validate the referral chain required for client access.

2. **Communication:** To establish an encrypted bridge for sensitive discussions.
3. **Defense:** To detect, investigate, and neutralize threats to our digital infrastructure (e.g., DDoS attacks, scanning, enumeration).

We explicitly disavow the following uses:

- We do not sell data to brokers.
- We do not share data with advertising networks.
- We do not use behavioral profiling for marketing.

4. DISCLOSURE & OPERATIONAL SHARING We maintain a "need-to-know" architecture. Your data is never disclosed to third parties, with the following strictly defined exceptions:

- **Operational Partners:** We may share technical telemetry with our upstream security providers (e.g., Managed DNS, DDoS mitigation partners) solely to maintain site availability.
- **Legal Compliance:** We will disclose information *only* if compelled by a valid, jurisdictionally appropriate court order, subpoena, or warrant. We challenge overbroad requests. We do not comply with informal law enforcement requests or "letters of request" lacking judicial force.
- **Exigent Circumstances:** We reserve the right to share information with relevant authorities if we have a good faith belief that there is an imminent, credible threat to the physical safety of a person (kinetic risk) or critical infrastructure.

5. DATA RETENTION & DESTRUCTION

- **Public Inquiries:** Data from unverified or rejected inquiries is purged from our active systems after 90 days.
- **Telemetry Logs:** Security logs are retained on a rolling 12-month basis for forensic readiness, then cryptographically shredded.

6. INTERNATIONAL DATA SOVEREIGNTY Our infrastructure is distributed. If you are accessing this Site from outside the United States, you acknowledge that your information may be transferred to, stored, and processed in the United States or secure offshore jurisdictions chosen for their strong privacy laws (e.g., Switzerland, Iceland). By using this Site, you consent to this transfer.

7. YOUR RIGHTS (GDPR / CCPA / CPRA) Regardless of your citizenship, we extend the following rights to all visitors to signal our commitment to privacy:

- **Right to Erase ("The Burn Notice"):** You may request the deletion of your personal data held in our public-facing systems.
- **Right to Know:** You may request a report on the specific data categories we have collected about you.
- **Non-Discrimination:** We will not deny services or degrade operational readiness based on your exercise of these rights.

To exercise these rights, submit a cryptographically signed request to the email address below.

8. SECURITY POSTURE We employ "Standard of Care" security measures appropriate for a high-threat environment, including but not limited to TLS 1.3 encryption for transit, zero-knowledge storage where applicable, and strict access controls. However, no transmission over the public internet is theoretically invulnerable. You engage with this Site at your own risk.

9. LINKS TO THIRD-PARTY INTELLIGENCE This Site may contain links to external intelligence sources or partners. We are not responsible for the hygiene or privacy practices of these external domains.

10. GOVERNING LAW This Policy and any disputes arising from it shall be governed by the laws of the **State of Montana**, without regard to its conflict of law principles. Any legal action must be brought exclusively in the courts located within Montana.

11. CONTACT & ENCRYPTED CHANNEL For privacy-related inquiries or to initiate a Right to Erase request:

Email: `privacy@conciergedefense.com`

PGP Key: `https://conciergedefense.com/pgp-key.txt`

Note: We do not accept service of process via email.