PRIVACY POLICY

Effective Date: December 2, 2025

Last Updated: December 2, 2025

1. INTRODUCTION AND SCOPE

Teisoft LLC ("Teisoft," "we," "us," or "our"), headquartered in Miami, Florida, is committed to safeguarding the privacy and security of your data. As a cybersecurity firm specializing in offensive validation and regulatory compliance (SOC2, PCI, HIPAA), we understand that confidentiality is the cornerstone of our business relationship.

This Privacy Policy outlines how we collect, use, and protect personal and operational information through our website (teisoftllc.com) and our services, including Continuous Penetration Testing, Phishing Awareness, and Secure Infrastructure Management.

2. INFORMATION WE COLLECT

We distinguish between two critical types of data:

A. Visitor & Marketing Data (Public Website)

- **Identity Information:** Name, job title, corporate email, and phone number collected through forms (e.g., "Book Your Validation Strategy").
- **Digital Footprint:** IP addresses, browser type, operating system, and navigation behavior.
- **Tracking Data:** We utilize third-party tracking tools, specifically **Google Analytics** and **LinkedIn Insights**, to analyze traffic patterns and ad performance.

B. Security Service Data (Client Operations)

In the course of delivering our services, we process:

- **Target Data:** IP ranges, URLs, system configurations, and cloud architecture diagrams (AWS) required for validation.
- **Workforce Data:** Employee names and email addresses provided strictly for authorized Phishing Simulations.
- **Vulnerability Findings:** Detailed reports on security flaws, exploits, and remediation status.

Note: *Security Service Data is primarily governed by the* ***specific Service Agreement*** *(e.g., Penetration Testing Agreement, Managed Infrastructure Agreement) and* ***Non-Disclosure Agreements (NDA)*** *signed with each client. In the event of a conflict regarding strict confidentiality of operational data, the terms of the signed Service Agreement shall take precedence over this policy.*

3. HOW WE USE YOUR INFORMATION

We use your data for the following legitimate business purposes:

- **Service Execution:** To perform penetration tests, phishing simulations, and infrastructure hardening as contracted.
- **Compliance Evidence:** To generate the audit logs and attestation reports required for your SOC2, PCI, or HIPAA validation.
- **Internal Training & QA:** To refine our adversarial methodologies and train our security teams. (See Section 6 for retention specifics).
- **Marketing Effectiveness:** To measure the performance of our LinkedIn campaigns and website user experience via Google Analytics.

4. COOKIES AND TRACKING TECHNOLOGIES

We use cookies to enhance your experience and analyze our traffic.

- **Google Analytics:** Used to understand how visitors interact with our site. You can opt-out using the [Google Analytics Opt-out Browser Add-on].
- **LinkedIn Insights Tag:** Used to track conversions and deliver targeted advertising to professional audiences. You can manage your LinkedIn ad preferences in your LinkedIn settings.
- **Control:** You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, some features of our Service may not function properly without cookies.

5. DATA SHARING AND DISCLOSURE

We do not sell your data. We do not process payments on this website; all invoicing is handled via external, secure channels. We share information only in the following limited circumstances:

- **Trusted Infrastructure Providers:** We use AWS and Microsoft Azure to host our secure platforms. These providers are contractually bound to maintain confidentiality.
- **Legal Requirements:** If required by a subpoena, court order, or government agency, strictly following a legal validation process.
- **Authorized Auditors:** We may share validation reports directly with your external auditors *only upon your explicit written instruction*.

6. DATA RETENTION POLICY

- **Marketing Data:** Retained as long as you maintain a relationship with us or until you request deletion.
- **Operational & Vulnerability Data:** Unless otherwise specified in a Services Agreement, Teisoft retains vulnerability reports and testing logs for a period of **one (1) year** following the conclusion of a project.
    - *Purpose:* This retention allows for year-over-year trend analysis, internal team training on complex exploit chains, and audit trail recovery if requested by the client.

  - *Security:* During this retention period, data remains encrypted and isolated in our secure evidence locker. After one year, data is securely destroyed or permanently anonymized.

7. DATA SECURITY

We apply "Security-First" standards to our own infrastructure:

- **Encryption:** All vulnerability data is encrypted at rest (AES-256) and in transit (TLS 1.3).
- **Access Control:** Access is restricted to authorized security personnel via strict Role-Based Access Control (RBAC) and mandatory Multi-Factor Authentication (MFA).
- **Payment Security:** We do not collect or store credit card information on our servers. All financial transactions are processed through compliant external invoicing systems.

8. YOUR RIGHTS

Depending on your jurisdiction, you have the right to:

- Request access to the personal data we hold about you.
- Request the correction or deletion of your data.
- Opt-out of marketing communications.

To exercise these rights, please contact our Compliance Officer at: [Insert Email]

9. CHANGES TO THIS POLICY

We reserve the right to update this policy. The most current version will always be available on our website.