IRON WARDEN LLC

Privacy Policy

Effective Date: February 13, 2026

Iron Warden LLC (“Iron Warden,” “we,” “our,” or “us”) is a cybersecurity consulting practice dedicated to safeguarding your privacy rights while delivering high-quality advisory services. This Privacy Policy outlines in detail our practices regarding the collection, use, disclosure, storage, and protection of personal information obtained through our website (https://ironwarden.org/), email communications, contact forms, video interviews, phone calls, questionnaires, and any other interactions related to our cybersecurity consulting services. This Policy applies to all individuals and entities who visit our website, inquire about our services, or engage us as clients (collectively, "you" or "users"). By accessing our website, submitting information, or utilizing our services, you acknowledge that you have read, understood, and consent to the practices described in this Policy.

We are based in Oklahoma, USA, and our operations are limited to serving clients within the United States. We strive to comply with applicable U.S. federal and state privacy laws, including but not limited to the Federal Trade Commission (FTC) Act, the Children's Online Privacy Protection Act (COPPA), the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) for California residents, and other relevant state data protection regulations such as those in Virginia (VCDPA), Colorado (CPA), Connecticut (CTDPA), and Utah (UCPA), where applicable. This Policy does not extend to information practices of third-party websites, applications, or services that may be linked from our site, over which we have no control.

If you are a resident of a jurisdiction with specific data protection laws (e.g., the European Union's General Data Protection Regulation (GDPR)), please note that we do not intentionally collect or process data from outside the U.S., and this Policy is not intended to comply with non-U.S. laws. If you access our services from outside the U.S., you do so at your own risk.

1. Information We Collect

We collect various types of information to provide, improve, and secure our services. The categories and sources of information include:

- **Personal Information You Provide Directly**: This is information you voluntarily submit to us, which may identify you individually or in combination with other data. Examples include:
    - Contact and identification details: Full name, company name, job title, email address, phone number, mailing address, and any other identifiers you provide.
    - Business-related information: Details about your organization, such as industry sector, business size (e.g., small business, sole proprietorship, large enterprise), cybersecurity needs, existing policies, vendor relationships, and responses to our questionnaires or interviews.

    - Service-specific data: Information shared during consultations, such as descriptions of your current security controls, documentation for review (e.g., contracts, policies), or details for assessments (e.g., vendor names for third-party risk evaluations).
    - Payment information: If applicable, billing details (e.g., credit card numbers, bank account information) processed through secure third-party payment gateways. We do not store payment card details directly.
- **Automatically Collected Information**: When you interact with our website or services, we may use automated technologies to gather non-personal or technical data for operational efficiency, security monitoring, and analytics. This includes:
    - Device and network information: IP address, browser type and version, operating system, device model, unique device identifiers (UDIDs), mobile network information, and internet service provider (ISP).
    - Usage and behavioral data: Pages visited, time and date of access, duration of sessions, referral sources (e.g., how you arrived at our site), clickstream data, search terms used on our site, and interaction patterns (e.g., form submissions).
    - Log and diagnostic data: Server logs, error messages, crash reports, and performance metrics to troubleshoot issues.
    - Location data: Approximate location derived from IP address (not precise geolocation unless you provide it).
- **Information from Third-Party Sources**: We may obtain supplementary data from reliable external sources to enhance our services or verify information:
    - Service providers: Data from tools we use, such as email delivery confirmations from platforms like Mailchimp or analytics insights from Google Analytics.
    - Public sources: For third-party risk assessments, we may review publicly available information about vendors (e.g., security breach reports from news sources or public databases).
    - Business partners: If you are referred to us, we may receive basic contact details from the referring party with your consent.

We minimize collection to what is necessary for our services and do not collect sensitive personal information (e.g., racial or ethnic origin, political opinions, religious beliefs, genetic or biometric data, health information, sexual orientation, or criminal records) unless it is explicitly provided by you and directly relevant to a service (e.g., in a HIPAA-related assessment). We do not collect or process information from individuals under the age of 18, and if we discover such collection, we will delete it immediately.

2. How We Use Your Information

We process your information for specific, legitimate purposes aligned with our business operations. Our uses are based on one or more legal bases, such as your consent, contractual necessity, compliance with legal obligations, or our legitimate interests (e.g., improving security or marketing our services). Specific uses include:

- **Service Provision and Fulfillment**: To respond to your inquiries, process service requests, schedule video interviews or calls, administer questionnaires, conduct assessments (e.g., pre-audit evaluations against standards like SOC 2, HIPAA, PCI DSS, ISO 27001), develop or review policies (e.g., Acceptable Use, Incident Response, Data Protection), perform risk assessments, and deliver reports with findings, scores, and recommendations.
- **Communication and Relationship Management**: To send service confirmations, updates, progress reports, final deliverables, invoices, and follow-up communications. We may also use your information to manage client relationships, such as sending reminders or seeking feedback.
- **Website and Service Improvement**: To analyze usage patterns, troubleshoot technical issues, enhance user experience, customize content, and develop new services based on aggregated, anonymized data.
- **Security and Risk Management**: To detect, prevent, and respond to security threats, fraud, unauthorized access, or violations of our Terms; to monitor for malicious activity; and to conduct internal audits.
- **Compliance and Legal Obligations**: To fulfill legal requirements, such as responding to subpoenas, court orders, or regulatory inquiries; to report data breaches if required; and to maintain records for tax, accounting, or dispute resolution purposes.
- **Marketing and Promotions**: With your explicit consent (e.g., via opt-in), to send newsletters, promotional offers, or information about related services. You can withdraw consent at any time without affecting the lawfulness of prior processing.
- **Research and Analytics**: To conduct internal research, generate insights on cybersecurity trends, and improve our methodologies using de-identified data.

We do not use your information for automated decision-making that produces legal effects or similarly significant impacts on you.

3. Sharing and Disclosure of Information

We prioritize confidentiality and do not sell, rent, trade, or otherwise monetize your personal information. Disclosures are limited to the following scenarios, with appropriate safeguards (e.g., data processing agreements):

- **Service Providers and Vendors**: We share information with trusted third parties who perform functions on our behalf, such as:
    - IT and hosting providers (e.g., website hosting, cloud storage like AWS).
    - Communication tools (e.g., email services, video conferencing like Zoom).
    - Analytics and security tools (e.g., Google Analytics for usage stats, security software for threat detection). These entities are bound by contracts requiring them to use data only for specified purposes, maintain confidentiality, and implement security measures.
- **Business Transfers or Reorganizations**: In the event of a merger, acquisition, bankruptcy, or sale of all or part of our assets, your information may be transferred to the new entity, provided they agree to equivalent privacy protections. We will notify you of such changes.
- **Legal and Regulatory Requirements**: We may disclose information if compelled by law, regulation, legal process (e.g., warrant, subpoena), or government request; to enforce our rights or defend against claims; to prevent harm or illegal activities; or in response to emergencies threatening safety.
- **Professional Advisors**: To auditors, accountants, legal counsel, or consultants for business purposes, under confidentiality obligations.
- **Aggregated or De-Identified Data**: We may share anonymized or aggregated data (from which you cannot be identified) for research, benchmarking, or statistical analysis with industry partners or publicly.

Since our services are U.S.-only, we do not transfer data internationally. If any service provider operates outside the U.S., we ensure adequate protections (e.g., Standard Contractual Clauses).

4. Data Security and Retention

Protecting your information is paramount. We employ a multi-layered approach to security:

- **Administrative Safeguards**: Policies and training for employees on data handling, access restrictions based on "need-to-know," and regular risk assessments.
- **Technical Safeguards**: Encryption for data in transit (e.g., TLS/SSL) and at rest; firewalls, intrusion detection systems; secure authentication (e.g., multi-factor); and regular vulnerability scanning and penetration testing.
- **Physical Safeguards**: Secure facilities for any physical records, though most operations are digital and remote.

Despite these measures, no system is infallible, and we cannot guarantee against all risks, such as sophisticated cyberattacks. In the event of a data breach, we will notify affected individuals and authorities as required by law (e.g., within 72 hours under certain state laws).

We retain information for the minimum period necessary:

- Service-related data: Up to 7 years post-service completion for legal, tax, and audit purposes.
- Website logs: Up to 2 years for security analysis.
- Marketing data: Until consent is withdrawn. After retention periods, we securely delete or anonymize data using industry-standard methods (e.g., overwriting, degaussing).

5. Cookies and Similar Tracking Technologies

Our website utilizes cookies, web beacons, pixels, and other tracking technologies to enhance functionality and gather insights:

- **Types of Cookies**:
    - Essential/Strictly Necessary: For core site operations, such as maintaining sessions and security features.
    - Performance/Analytics: To measure traffic, engagement, and effectiveness (e.g., Google Analytics cookies tracking anonymous usage).
    - Functionality: To remember preferences (e.g., language settings, if implemented).
    - We do not use targeting or advertising cookies, as we do not engage in behavioral advertising.
- **Management Options**: You can control cookies via browser settings (e.g., block or alert), use "Do Not Track" (DNT) signals (which we honor where possible), or opt-out tools from providers like Google. Note that disabling cookies may impair site functionality.

We do not track users across third-party sites.

6. Your Privacy Rights and Choices

We respect your control over your information. Depending on your jurisdiction, you may have the following rights:

- **Access**: Request details about the personal information we hold about you.
- **Correction/Rectification**: Update inaccurate or incomplete data.
- **Deletion/Erasure**: Request removal of your data, subject to legal retention requirements.
- **Restriction/Objection**: Limit processing or object to certain uses (e.g., marketing).
- **Portability**: Receive your data in a structured, machine-readable format.

- **Opt-Out of Sale/Sharing**: Though we do not sell data, California residents can opt-out of any sharing for targeted advertising (not applicable here).
- **Non-Discrimination**: We will not discriminate against you for exercising rights.

To exercise rights, submit a verifiable request via email to jimmy@ironwarden.org. We will respond within the legally required timeframe (e.g., 45 days for CCPA, extendable to 90 days). Verification may include matching provided details to our records. If denied, we will explain why and provide appeal options.

You can also:

- Opt-out of marketing emails by clicking "unsubscribe" links.
- Withdraw consent at any time, though this may limit services.

7. Children's Privacy

Our website and services are not intended for children under 18. We do not knowingly collect personal information from minors. If we become aware of such collection (e.g., via parental notification), we will promptly delete the data and terminate any associated account. Parents or guardians can contact us for assistance.

8. Data Breach Notification

In the unlikely event of a security incident compromising personal information, we will notify you without undue delay if required by law (e.g., if there's a risk of harm). Notifications will include details of the breach, affected data, mitigation steps, and protective advice.

9. Third-Party Practices

Our site may include links to external resources (e.g., standards bodies like NIST). We are not responsible for their privacy practices. Review their policies before interacting.

10. Changes to This Privacy Policy

We may revise this Policy to reflect changes in our practices, technologies, legal requirements, or services. Updates will be posted prominently on our website with a revised effective date and, where material, notified via email. Your continued use after changes constitutes acceptance. We recommend reviewing this Policy periodically.

11. Contact Us

For any questions, concerns, requests, or complaints about this Policy or our data practices:

Iron Warden LLC

Email: jimmy@ironwarden.org

Phone: (918) 308-9484

Location: Oklahoma, USA

If unsatisfied with our response, you may contact your state Attorney General, the FTC (ftc.gov/complaint), or other relevant authorities. California residents can contact the California Privacy Protection Agency.