



ENTRYPOINT

— RISK STRATEGIES —

CLEAR DIRECTION. SMARTER DECISIONS. STRONGER OUTCOMES.

PUBLIC WEBSITE POLICY

Website Privacy Policy

Transparent data practices for a low-collection public website.

This Policy explains the limited information processed through EntryPoint's public website, voluntary email contact, hosting environment, and ordinary security operations.

EFFECTIVE DATE May 25, 2026	LAST UPDATED July 15, 2026
WEBSITE entrypoint-strategies.com	DOCUMENT OWNER EntryPoint Strategies LLC

Clear direction. Smarter decisions. Stronger outcomes.



Document Overview

DOCUMENT TYPE	Public-facing website policy
APPLIES TO	entrypoint-strategies.com, website CTAs, the interactive diagnostic, and related pre-engagement communications
LEGAL ENTITY	EntryPoint Strategies LLC, d/b/a EntryPoint Risk Strategies

Use note: This policy governs the public website only. A signed client agreement, Statement of Work, or data-handling addendum controls any professional engagement.

Contents

01 Scope of This Policy	14 HIPAA and Healthcare Information
02 Summary of Current Website Practices	15 Payment Information
03 Information You Voluntarily Provide	16 Data Retention
04 Interactive Diagnostic Information	17 Data Security
05 Information Processed Automatically	18 Your Privacy Choices and Rights
06 Cookies and Similar Technologies	19 Submitting a Privacy Request
07 How EntryPoint Uses Information	20 California and Other U.S. State Disclosures
08 Email and Marketing Communications	21 Visitors Outside the United States
09 No Sale or Targeted-Advertising Sharing	22 Children's Privacy
10 When Information May Be Disclosed	23 Third-Party Links
11 Hostinger Hosting Environment	24 Changes to This Privacy Policy
12 International Processing	25 Contact Information
13 Restricted and Sensitive Information	



Entrypoint Strategies LLC, doing business as Entrypoint Risk Strategies ("Entrypoint," "we," "us," or "our"), respects the privacy of visitors to entrypoint-strategies.com.

This Privacy Policy explains what information may be collected when you visit the Website or voluntarily contact Entrypoint, how the information is used and protected, when it may be disclosed, and what choices may be available to you.

1. Scope of This Policy

This Policy applies to personal information processed through:

- The public Entrypoint website;
- Website call-to-action links;
- Emails sent in response to or through the Website;
- The Website's interactive diagnostic; and
- Related communications concerning a possible business relationship.

This Policy does not govern information processed under a signed client agreement, Statement of Work, Business Associate Addendum, regulated-data addendum, employment relationship, or contractor relationship when a separate agreement or notice applies.

2. Summary of Current Website Practices

The current Website:

- Does not require visitors to create an account;
- Does not provide a public client portal;
- Does not directly process payments;
- Does not intentionally collect passwords or authentication information;
- Does not intentionally collect protected health information or other regulated client records;
- Does not currently use optional advertising or behavioral-tracking technologies;
- Does not sell personal information;
- Does not share personal information for cross-context behavioral advertising;
- Does not operate as a data broker; and
- Receives identifying information primarily when a visitor voluntarily contacts Entrypoint.

As of the Last Updated date, the public Website does not require an account, registration, or a public contact-form submission. If you choose to contact Entrypoint, we receive the information you include in your email or other direct communication. Our hosting, email, and security providers also necessarily process limited technical information to deliver, maintain, and protect the Website and our communications.

3. Information You Voluntarily Provide

Entrypoint may collect information that you voluntarily provide when you email us, respond to a communication, request information, or discuss a potential engagement.

This may include:

- Your name;
- Email address;
- Telephone number, if you provide it;
- Business name;



-
- Job title or professional role;
 - Business location;
 - General industry or business category;
 - Information about your business stage;
 - General descriptions of security, vendor, policy, insurance, access, or documentation concerns;
 - Scheduling information;
 - The contents of your message; and
 - Other information you choose to provide.

Please provide only the minimum information necessary to explain your inquiry.

4. Interactive Diagnostic Information

The Website may provide an interactive diagnostic that asks you to select general information about:

- Your type of business;
- Your stage of development;
- The business pressure or concern that feels most urgent; and
- The area in which you may need guidance.

The diagnostic does not require you to enter your name, email address, credentials, client records, or other direct identifiers.

Your selections may be temporarily processed within your browser to display a general recommended starting point. EntryPoint does not intentionally use these selections to identify you or create a persistent personal profile.

If EntryPoint later changes the diagnostic so that responses are transmitted, retained, linked to contact information, or used for analytics, this Policy will be updated before that new use begins.

5. Information Processed Automatically

Even when you do not voluntarily contact EntryPoint, the Website's hosting environment may process standard technical information needed to deliver, secure, and maintain the Website.

Depending on the hosting configuration, this information may include:

- Internet Protocol address;
- Browser type and version;
- Device type;
- Operating system;
- Referring page or domain;
- Pages or resources requested;
- Date and time of a request;
- General geographic region inferred from an IP address;
- Error, diagnostic, and performance information; and
- Security events, blocked requests, or suspected malicious activity.

This information is generally processed through ordinary server, hosting, content-delivery, and security logs. EntryPoint does not intentionally use these logs to create advertising profiles or identify ordinary visitors by name.



6. Cookies and Similar Technologies

Current Configuration

The Website is hosted using Hostinger hosting infrastructure. EntryPoint has not enabled optional analytics, advertising, session-replay, retargeting, or cross-site behavioral-tracking integrations through the Website.

EntryPoint has not intentionally enabled tools such as:

- Google Analytics;
- Meta Pixel;
- Hotjar;
- Advertising-network pixels; or
- Third-party behavioral profiling tools.

The Website may use strictly necessary technical storage if required for security, site delivery, accessibility, user preferences, or similar essential functions. Ordinary server logging is not the same as placing an advertising cookie on your device.

Future Changes

Before enabling a non-essential analytics, advertising, personalization, or tracking technology, EntryPoint will:

- Evaluate the information the technology collects;
- Update this Privacy Policy;
- Update its vendor and data-processing records;
- Configure an appropriate cookie or consent mechanism where required;
- Prevent optional tracking from loading before consent where required; and
- Provide an appropriate method to withdraw or change consent.

Browser Controls

You can configure your browser to block or delete cookies. Blocking essential storage may affect the operation of some website features.

Do Not Track and Global Privacy Control

Because EntryPoint does not currently enable cross-site advertising or behavioral tracking on this Website, the Website does not respond differently to browser Do Not Track signals at this time.

EntryPoint does not knowingly permit non-essential third parties to collect personal information about your online activities over time and across different websites through this Website. Hosting and infrastructure providers may still receive technical request information needed to deliver, secure, and maintain the Website. Where applicable law requires recognition of a legally valid universal opt-out signal, such as Global Privacy Control, EntryPoint will process the signal as required.

7. How EntryPoint Uses Information

EntryPoint may use personal information to:

- Respond to questions or requests;
- Communicate about EntryPoint's services;
- Determine whether a proposed engagement may be a suitable fit;
- Schedule and conduct introductory conversations;
- Prepare a requested proposal or scope discussion;



-
- Maintain records of inquiries and business communications;
 - Provide requested follow-up information;
 - Protect the Website, email environment, accounts, and operations;
 - Detect spam, abuse, fraud, or malicious activity;
 - Investigate errors or security events;
 - Comply with legal, regulatory, tax, accounting, or recordkeeping obligations;
 - Establish, exercise, or defend legal claims;
 - Enforce applicable agreements and Website Terms; and
 - Carry out another purpose disclosed at the time the information is provided.

EntryPoint may also use information with your consent.

8. Email and Marketing Communications

When you voluntarily contact EntryPoint, we may reply concerning your inquiry, a requested conversation, or a possible business relationship.

Submitting an inquiry does not automatically subscribe you to a recurring newsletter or unrelated promotional mailing list.

EntryPoint may send lawful business-development or follow-up communications where permitted. If EntryPoint sends marketing emails, those messages will use accurate sender information, include EntryPoint's valid postal mailing address and a clear opt-out method, and identify commercial content as required by applicable law.

EntryPoint will honor opt-out requests within the time required by applicable law.

You may opt out by:

- Using an unsubscribe method included in the communication, if available; or
- Emailing contact@entrypoint-strategies.com with the subject line "Unsubscribe."

EntryPoint may retain limited information necessary to honor an opt-out request.

9. No Sale or Targeted-Advertising Sharing

EntryPoint does not sell, rent, or license personal information to third parties.

EntryPoint does not currently:

- Share personal information for cross-context behavioral advertising;
- Use personal information collected through this Website for targeted advertising;
- Receive payment for disclosing Website visitor information;
- Operate a data-broker business; or
- Offer a financial incentive in exchange for personal information.

If these practices change, EntryPoint will update this Policy and provide any notice, consent, or opt-out mechanism required by applicable law before the new practice begins.

10. When Information May Be Disclosed

EntryPoint may disclose information in the following limited circumstances.



Hosting and Infrastructure Providers

The Website is hosted using Hostinger. Hostinger may process Website content, requests, IP addresses, technical logs, security information, and related data as necessary to provide hosting, infrastructure, maintenance, fraud prevention, and security services.

Business Email and Productivity Providers

When you email EntryPoint, your communication may be processed through EntryPoint's business email, storage, security, and productivity providers, including Google Workspace or a replacement business provider.

Contractors and Professional Service Providers

Information may be provided to authorized contractors, consultants, accountants, attorneys, insurers, security providers, or other professional advisors who have a legitimate need for the information and are subject to appropriate confidentiality or professional obligations.

Legal and Safety Requirements

EntryPoint may disclose information when it reasonably believes disclosure is necessary to:

- Comply with law, regulation, subpoena, court order, or lawful governmental request;
- Protect the rights, safety, property, systems, or operations of EntryPoint or another person;
- Investigate suspected fraud, abuse, malicious activity, or a security event;
- Enforce a contract or these Website Terms; or
- Establish, exercise, or defend legal claims.

Business Transactions

Information may be transferred as part of a merger, acquisition, financing, reorganization, sale of assets, or similar transaction, subject to appropriate confidentiality and legal requirements.

EntryPoint does not authorize service providers to use Website personal information for their independent targeted advertising. Where appropriate, EntryPoint uses service providers under contracts or arrangements designed to limit processing to authorized purposes and support reasonable security for the limited personal information involved.

11. Hostinger Hosting Environment

Hostinger Website Builder provides the hosting infrastructure used to make the Website publicly available.

As part of this role, Hostinger may process technical and operational information on EntryPoint's behalf. This may include IP addresses, request records, browser or device information, security events, error information, and related hosting data.

EntryPoint is responsible for determining why personal information is processed through its Website. Hostinger and other infrastructure providers may act as service providers or processors when handling information on EntryPoint's behalf.

Hostinger may use data centers, affiliates, or subprocessors located in the United States or other countries. Their processing is also governed by their applicable agreements, privacy terms, and security practices.

The current EntryPoint CTA is intended to direct visitors to email EntryPoint. It is not intended to store a contact-form submission in a Website account or public-facing database. If EntryPoint later adds a native form, newsletter field, analytics tool, advertising pixel, chat feature, scheduling embed, or similar integration, this



Policy and any required point-of-collection or consent notice will be updated before or when the new processing begins.

12. International Processing

EntryPoint is based in the United States. Personal information may therefore be processed in the United States and in other countries where EntryPoint's hosting, email, security, or service providers operate.

Those countries may have privacy laws that differ from the laws where you live.

Where applicable law requires a transfer mechanism or additional safeguard, EntryPoint will use an appropriate contractual or legal mechanism.

13. Restricted and Sensitive Information

The public Website and ordinary email are not approved channels for restricted or highly sensitive information.

Do not provide:

- Passwords;
- MFA codes or recovery codes;
- Authentication tokens;
- Private keys or seed phrases;
- Social Security numbers;
- Full dates of birth;
- Government identification numbers;
- Bank-account credentials;
- Full payment-card information;
- Protected health information;
- Patient records;
- Unredacted tax or payroll records;
- Privileged legal communications;
- Legal case files;
- Classified or export-controlled information;
- Production datasets;
- Detailed exploitable vulnerability information; or
- Information you are not authorized to disclose.

If restricted information is necessary for a potential client engagement, do not provide it unless and until EntryPoint has established an appropriate written scope, authorized data categories, secure-transfer method, retention period, and any legally required agreement, Business Associate Addendum, or similar data-handling addendum.

EntryPoint may delete, quarantine, return, or decline to review unauthorized restricted information.

14. HIPAA and Healthcare Information

The Website is not a patient portal, clinical communication system, or approved method for submitting protected health information.

A visitor's general inquiry about healthcare cybersecurity does not, by itself, make EntryPoint a business associate under HIPAA.



Do not send patient names, medical records, treatment information, medical-record numbers, billing records containing patient identifiers, or other protected health information through the Website or ordinary email.

If a future engagement requires EntryPoint to create, receive, maintain, or transmit protected health information on behalf of a HIPAA covered entity or business associate, do not send the information unless and until the parties establish the necessary written scope and execute any required Business Associate Agreement, Business Associate Addendum, or similar HIPAA-related agreement.

15. Payment Information

The public Website does not directly collect payment-card information.

Client payments may be handled by an independent third-party payment processor after a written engagement is established. EntryPoint does not intend to receive full card numbers, security codes, PINs, magnetic-stripe data, chip data, or payment-authentication information.

The payment processor's privacy policy and terms apply to information submitted directly to that processor.

16. Data Retention

EntryPoint retains personal information only for as long as reasonably necessary for the purposes described in this Policy and consistent with applicable legal, accounting, security, and recordkeeping needs.

Business inquiry emails and related contact details that do not become a client engagement are generally retained for up to 24 months after EntryPoint's last substantive contact, unless a longer period is reasonably necessary for legal, accounting, security, dispute-resolution, suppression-list, contractual, or recordkeeping purposes.

If an inquiry develops into a client engagement, retention of engagement records is governed by the applicable agreement, EntryPoint's records practices, and legal or professional obligations.

Technical server, security, and backup records are retained according to EntryPoint's providers' operational, backup, security, and contractual practices. If a stricter retention disclosure is required by applicable law, EntryPoint will provide it at or before the point of collection.

17. Data Security

EntryPoint uses administrative, technical, and physical safeguards designed to be appropriate to the sensitivity of the limited personal information received through the Website.

These safeguards are designed to include measures such as:

- Encrypted Website connections;
- Access controls for the business systems used to receive and manage inquiries;
- Security features provided by EntryPoint's hosting, email, and other service providers;
- Data-minimization and authorized-access practices; and
- Incident-response and legally required notification processes.

EntryPoint may update its safeguards over time and does not publicly describe every security control it uses.

No website, email provider, transmission method, or storage system can be guaranteed completely secure. Do not send information through the Website or ordinary email when the risk of interception or unauthorized access is unacceptable.



If EntryPoint discovers a security event involving personal information for which notice is required, EntryPoint will provide notice in accordance with applicable law.

18. Your Privacy Choices and Rights

Depending on where you live and to the extent a particular privacy law applies, you may have the right to:

- Ask whether EntryPoint processes personal information about you;
- Request access to personal information;
- Request correction of inaccurate information;
- Request deletion of information;
- Obtain a portable copy of certain information;
- Withdraw consent where processing is based on consent;
- Object to or restrict certain processing;
- Opt out of targeted advertising;
- Opt out of the sale of personal information;
- Opt out of certain profiling activities;
- Limit certain uses of sensitive personal information;
- Appeal the denial of a privacy request; and
- Complain to an appropriate regulatory authority.

Because EntryPoint does not currently sell personal information or use it for targeted advertising, some opt-out rights may not apply to the current Website practices.

EntryPoint may voluntarily consider a reasonable access, correction, or deletion request even when a specific state privacy statute does not apply.

19. Submitting a Privacy Request

Privacy requests may be sent to contact@entrypoint-strategies.com. Use the subject line “Privacy Request” and describe the right you wish to exercise.

EntryPoint may need to verify your identity before completing a request. Verification may involve confirming control of the email address associated with the information or requesting additional limited information.

EntryPoint will use information submitted for verification only to evaluate and respond to the request.

EntryPoint may deny or limit a request when permitted by law, including when:

- Identity cannot reasonably be verified;
- The request is fraudulent, abusive, or excessive;
- Retention is required by law or contract;
- The information is necessary for security or fraud prevention;
- The information is needed to establish or defend legal claims;
- Deletion would affect another person’s rights; or
- An applicable exception applies.

EntryPoint will respond within the period required by applicable law.

Where a right to appeal applies, send an email with the subject line “Privacy Appeal” and explain why you believe the decision should be reconsidered.

Authorized agents may submit requests where applicable law permits, but EntryPoint may require proof of authorization and direct verification from the individual.



EntryPoint will not unlawfully discriminate against you for exercising a privacy right. Privacy requests are handled only to the extent applicable law requires, although EntryPoint may voluntarily consider reasonable requests when a specific statute does not apply.

20. California and Other U.S. State Disclosures

For purposes of U.S. state privacy laws that may apply, EntryPoint may have processed the following categories of personal information during the preceding twelve months:

Identifiers

Examples include a name, email address, business contact information, IP address, or similar identifier.

Sources include information provided directly by visitors and information generated through ordinary Website infrastructure.

Professional or Business Information

Examples include business name, job title, industry, business stage, and general business concerns.

Sources include information voluntarily provided by visitors.

Communications

Examples include emails, inquiry contents, scheduling communications, and related records.

Sources include direct communications with visitors.

Internet or Electronic Network Activity

Examples include browser type, device type, requested pages, referring page, timestamps, and security-log information.

Sources include the visitor's browser, device, hosting provider, and security infrastructure.

EntryPoint uses these categories for the purposes described in this Policy and may disclose them to service providers, professional advisors, or government authorities in the limited circumstances described above. If applicable law requires a more specific notice at collection or category-level retention disclosure, EntryPoint will provide that notice at or before the relevant collection.

During the preceding twelve months, EntryPoint has not intentionally:

- Sold personal information;
- Shared personal information for cross-context behavioral advertising;
- Used Website information for targeted advertising;
- Offered financial incentives for personal information; or
- Intentionally collected sensitive personal information through the public Website.

EntryPoint does not knowingly permit third parties to collect personally identifiable information through the Website for independent behavioral advertising.

21. Visitors Outside the United States

If privacy law in your jurisdiction applies to EntryPoint's processing, the legal basis may include:

- Your consent;
- Steps taken at your request before entering a contract;



-
- Entrypoint's legitimate interest in responding to business inquiries and operating a secure Website;
 - Performance of a contract;
 - Compliance with a legal obligation; or
 - Establishment, exercise, or defense of legal claims.

You may have the right to contact your local data-protection authority. Entrypoint encourages you to contact Entrypoint first so that the concern can be reviewed directly.

22. Children's Privacy

The Website is intended for adults and businesses. It is not directed to children under thirteen and is not designed to collect personal information from children.

Entrypoint does not knowingly collect personal information from children under thirteen through the Website.

If Entrypoint learns that a child under thirteen has provided personal information through the Website, Entrypoint will investigate and delete the information as required by applicable law.

23. Third-Party Links

The Website may contain links to external websites or services.

Entrypoint does not control the privacy, security, accessibility, content, or data-handling practices of third parties. Review the privacy policy of an external service before providing it with information.

24. Changes to This Privacy Policy

Entrypoint may update this Policy when:

- Website functionality changes;
- New vendors or integrations are added;
- Analytics, cookies, or advertising technologies are enabled;
- Contact or intake workflows change;
- Business operations change; or
- Legal requirements change.

The revised Policy will be posted with an updated date.

If a change materially affects how previously collected personal information is used, Entrypoint will provide additional notice or obtain consent where required.



25. Contact Information

Questions, concerns, and privacy requests may be directed to:

ENTRYPOINT STRATEGIES LLC

d/b/a EntryPoint Risk Strategies

2704 Amber Crest Rd
Hanover, Maryland 21076

706-513-6740

contact@entrypoint-strategies.com

entrypoint-strategies.com