PRIVACY POLICY

Effective Date: September 21, 2026

CrisisRisk Strategies, LLC ("CrisisRisk," "we," "us," or "our") respects the privacy and confidentiality of personal information entrusted to us.

This Privacy Policy explains how CrisisRisk collects, uses, stores, discloses, and protects personal information in connection with www.crisisrisk.com, our professional services, crisis-response services, Threat of Violence Questionnaires and assessments, training and risk-management resources, restricted-access toolkits, communications, and related activities.

CrisisRisk is a United States company. We provide services to insurers, insurance brokers and agents, insured organizations, prospective clients, and other organizations in the United States and internationally. As a result, personal information concerning individuals outside the United States may be transferred to, processed, and maintained in the United States.

This Privacy Policy is intended to provide information concerning our privacy practices, including information relevant to individuals in the European Economic Area ("EEA"), United Kingdom, Singapore, and Australia.

Information received in connection with a particular insurance policy, claim, crisis event, professional engagement, or other client matter may also be governed by contractual, insurance, confidentiality, legal, regulatory, or professional obligations.

1. Information We Collect

The information CrisisRisk collects depends upon the nature of your interaction with us.

We may collect, receive, maintain, or generate:

Depending upon the circumstances, some of this information may constitute sensitive information or special-category personal data under applicable privacy laws.

- Name and contact information, including email address, telephone number, and mailing address
- Employer, company, organization, and professional information
- Job title or professional role
- Information submitted through website forms
- Account, authentication, login, and restricted-resource access information
- Electronic license acceptance, checkbox, signature, and related records
- Date, time, IP address, login activity, and other technical or audit information associated with an account or restricted resource
- Communications with CrisisRisk
- Webinar and training registration information
- Threat of Violence Questionnaire, survey, and assessment information
- Risk-management and organizational preparedness information
- Crisis-response and incident information
- Insurance, policy, claim, and coverage-related information
- Information concerning employees, witnesses, victims, alleged perpetrators, family members, and other individuals
- Information concerning injuries, medical conditions, counseling needs, or other health-related matters when relevant to a crisis or claim

- Information concerning alleged or actual criminal conduct, threats, violence, investigations, litigation, or legal proceedings
- Technical information associated with use of our website
- Other information voluntarily provided to CrisisRisk or provided to us in connection with our services

2. Where We Obtain Personal Information

CrisisRisk may obtain personal information:

We may therefore hold personal information about an individual even when that individual did not provide the information directly to CrisisRisk.

- Directly from you
- From an insured organization
- From an insurer, reinsurer, insurance broker, or insurance agent
- From an employer or other organization
- Through CrisisRisk.com
- Through account creation or access to restricted resources
- Through a CrisisRisk questionnaire, survey, assessment, or communication
- Through Jotform or another platform used to administer a CrisisRisk questionnaire or assessment
- During a crisis-response call
- Through our answering service
- From attorneys, counselors, investigators, consultants, security professionals, or other professionals involved in a matter
- From witnesses, victims, employees, family members, or other individuals
- From publicly available sources
- From other sources when reasonably necessary to provide our services

3. CrisisRisk.com

CrisisRisk.com provides information about CrisisRisk and its services and provides access to certain forms, resources, and restricted-access materials.

The website is hosted through DreamHost and uses WordPress.

When you use our website, CrisisRisk and its technology providers may process technical information such as:

This information may be used to operate, maintain, secure, troubleshoot, administer, and improve the website and its restricted-access resources.

- Internet Protocol (“IP”) address
- Browser and device type
- Operating system
- Date and time of access
- Pages requested or viewed
- Referring website
- Technical log information
- Login and authentication information
- General website interaction information

4. Website Inquiries and "Ask an Expert"

When an individual submits an inquiry through CrisisRisk.com, including through our "Ask an Expert" functionality, we may collect the information provided in the form and any information included in the inquiry.

Ask an Expert communications are distributed to dwp@crisisrisk.com, which is a CrisisRisk distribution email accessible by designated CrisisRisk personnel.

Information submitted through this function is used to review and respond to the inquiry and, where appropriate, provide CrisisRisk services.

5. Registered Users and Restricted Resources

Certain CrisisRisk resources are available only to approved users, including insurance-company clients, insurance agents or brokers, insured organizations, and other authorized users.

CrisisRisk may collect or receive information necessary to establish an account and determine whether an individual or organization is authorized to access these resources.

CrisisRisk may approve, restrict, suspend, or terminate access based upon the individual's relationship with CrisisRisk, an insurer, broker, insured organization, applicable insurance program, license agreement, or other basis for authorized access.

6. Restricted-Access Toolkits and Risk-Management Resources

CrisisRisk maintains certain restricted-access webpages and resources on CrisisRisk.com that provide proprietary risk-management tools, templates, guidance, training materials, and other resources.

These include, among other resources, toolkits relating to California SB 553 and the United Kingdom's Terrorism (Protection of Premises) Act 2025, commonly known as Martyn's Law.

Authorized users may obtain access to these resources directly through CrisisRisk or may be directed to them through an insurer or other authorized platform, including the Beazley portal. The applicable toolkits and materials are hosted by CrisisRisk on CrisisRisk.com.

User Accounts and License Agreements

Because these materials are proprietary and licensed for authorized use, users are required to establish an account and accept or electronically sign an applicable license agreement before access is provided.

In connection with establishing and administering an account, granting access to licensed materials, and documenting the applicable license agreement, CrisisRisk may collect, maintain, or generate information including:

- Name
- Business email address
- Company or organization
- Job title or professional role
- Username, login credentials, or other account identifiers
- Relationship to an insurer, broker, insured organization, or other entity through which access is authorized
- Electronic acceptance, checkbox, signature, or other record demonstrating agreement to applicable licensing terms

- Date and time associated with account creation, acceptance of licensing terms, and access to resources
- Internet Protocol ("IP") address
- Login and access activity
- Information concerning the resource or toolkit accessed
- Other technical, security, authentication, or audit information generated in connection with the account or use of the restricted-access resources

Not every category of information listed above is necessarily collected during every interaction. The information collected may depend upon the particular resource, account functionality, technology in use, and method through which access is provided.

CrisisRisk may use this information to:

- Establish and administer user accounts
- Verify a user's identity, organization, or eligibility for access
- Authenticate users and provide access to restricted resources
- Administer and document applicable license agreements
- Maintain records of electronic acceptance or signature
- Protect CrisisRisk's proprietary and intellectual-property rights
- Prevent or investigate unauthorized access, reproduction, distribution, or use
- Maintain the security and integrity of CrisisRisk systems and resources
- Provide technical or administrative support
- Communicate with authorized users concerning the resources
- Maintain appropriate business, contractual, security, and legal records
- Establish, exercise, or defend contractual or legal rights

Where access is provided in connection with an insurance program, CrisisRisk may receive information from the applicable insurer, broker, agent, or insured organization to establish or verify that the individual or organization is eligible to access the resource.

Use of the Toolkits

Users generally access or download the tools and resources from CrisisRisk.com. Unless expressly provided otherwise for a particular service, users do not submit their completed versions of the toolkit documents to CrisisRisk through the restricted-access toolkit webpages.

The toolkits and other resources are intended to assist organizations with risk-management, planning, and compliance activities. Their availability or use does not constitute a representation or guarantee that an organization complies with any particular law, regulation, standard, or legal obligation.

7. Threat of Violence Questionnaires, Surveys, and Assessments

CrisisRisk provides Threat of Violence Questionnaires, surveys, and related assessments to help organizations evaluate violence-prevention preparedness, inherent risk, and related risk-management practices.

These questionnaires are not completed through CrisisRisk.com. CrisisRisk currently uses Jotform to administer and collect questionnaire and survey responses, including responses from organizations located outside the United States.

Depending upon the questionnaire or engagement, information collected may include:

CrisisRisk receives and retains questionnaire responses and uses them to perform assessments, prepare reports, provide recommendations, benchmark preparedness, and deliver related professional services.

Access within CrisisRisk to questionnaire information is limited based upon business need, with primary access restricted to designated personnel.

CrisisRisk does not sell questionnaire information or use individual questionnaire responses for unrelated third-party marketing.

Jotform separately processes information through its platform in accordance with the arrangements applicable to that service.

- Organization and respondent information
- Information concerning policies and procedures
- Emergency-response practices
- Security measures
- Behavioral threat assessment and management practices
- Human-resources practices
- Training practices
- Crisis-management and communications practices
- Information regarding violence-related exposures
- Other risk-management and preparedness information

8. Crisis-Response Calls and Answering Service

CrisisRisk provides 24-hour crisis-response services.

Calls may initially be answered by Specialty Answering Service ("SAS"), a third-party answering service used by CrisisRisk.

SAS may record the call and collect information necessary to identify the caller and facilitate an appropriate CrisisRisk response. This may include:

SAS may transfer the caller directly to CrisisRisk and may send designated CrisisRisk personnel text-message and email alerts containing relevant caller and incident information.

- Organization name
- Caller name
- Email address
- Telephone number
- Brief description of the reason for the call

9. Sensitive Information Received During Crisis Response

Crisis-response services may involve highly sensitive circumstances.

Depending upon the incident, CrisisRisk may receive information concerning:

CrisisRisk collects, uses, and discloses this information only as reasonably necessary in connection with the applicable crisis, claim, professional engagement, legal obligation, or other legitimate purpose.

- Employees
- Victims
- Witnesses
- Alleged perpetrators

- Family members
- Minors
- Injuries or deaths
- Physical or mental health conditions
- Counseling needs
- Threats or threatening behavior
- Alleged or actual criminal conduct
- Workplace or domestic violence
- Law-enforcement activity
- Investigations
- Insurance claims
- Litigation or anticipated litigation
- Legal advice or legal proceedings
- Security vulnerabilities
- Other sensitive circumstances surrounding an incident

10. How Crisis-Response Information May Be Used and Shared

Depending upon the circumstances, CrisisRisk may share relevant crisis-response information with parties involved in responding to or managing an incident, including:

CrisisRisk seeks to limit disclosures to information reasonably necessary for the applicable purpose.

- The applicable insured organization
- Insurers or reinsurers
- Insurance brokers or agents
- Attorneys or law firms
- Counselors or counseling providers
- Investigators
- Security or crisis-management professionals
- Other consultants or specialists
- Governmental, emergency-response, or law-enforcement authorities when appropriate or required
- Other parties when reasonably necessary to protect individuals, respond to an emergency, administer an insurance matter, provide professional services, or comply with law

11. How We Use Personal Information

- Provide CrisisRisk services
- Respond to inquiries
- Provide crisis-response services
- Coordinate emergency and professional resources
- Conduct Threat of Violence Questionnaires and assessments
- Prepare reports and recommendations
- Provide risk-management guidance
- Provide training and educational resources
- Establish and administer accounts
- Administer license agreements and restricted-access resources
- Protect proprietary resources and intellectual property

- Communicate with clients, insureds, insurers, brokers, and other business partners
- Manage insurance-related services
- Support claims, investigations, or litigation
- Protect individuals and organizations
- Maintain business and professional records
- Operate and secure our website and technology
- Prevent fraud, misuse, and unauthorized access
- Comply with contracts, laws, regulations, court orders, or legal process
- Establish, exercise, or defend contractual or legal rights
- Send permitted professional and marketing communications
- Perform other legitimate activities related to our professional services

12. Legal Bases for Processing — EEA and United Kingdom

Where the EU GDPR or UK GDPR applies, CrisisRisk processes personal data only where an appropriate legal basis exists.

Depending upon the processing activity and circumstances, our legal bases may include:

Performance of a contract or steps related to a contract. We may process personal data when necessary to provide requested services, administer an account or license, or perform contractual obligations.

Legitimate interests. We may process personal data when necessary for legitimate interests pursued by CrisisRisk or another party, provided those interests are not overridden by the individual's applicable rights and interests. These interests may include providing and improving risk-management and crisis-response services; protecting people and organizations; administering client, insurance, account, and licensing relationships; protecting proprietary resources; maintaining security; preventing misuse; and establishing or defending legal rights.

Compliance with legal obligations. We may process information where necessary to comply with an applicable legal obligation.

Vital interests. In an emergency or other appropriate circumstance, processing may be necessary to protect an individual's life, health, safety, or other vital interests.

Consent. Where required or appropriate, CrisisRisk may process personal data based upon an individual's consent. Where consent is the legal basis, the individual may withdraw that consent as permitted by applicable law.

The appropriate legal basis depends upon the particular processing activity and relationship involved.

13. Special-Category, Sensitive, and Criminal-Offence Information

Some CrisisRisk services may involve information that receives additional protection under applicable privacy laws, including health information and information concerning alleged or actual criminal conduct.

Where the EU GDPR or UK GDPR applies and CrisisRisk processes special-category personal data or criminal-offence information, CrisisRisk will rely upon an applicable legal basis and any additional condition required by applicable law.

Depending upon the circumstances, processing may relate to matters such as legal claims, protection of vital interests, substantial public interests recognized by applicable law, explicit consent where appropriate, or other legally permitted grounds.

Because the appropriate condition depends upon the facts and jurisdiction involved, CrisisRisk does not rely upon a single processing condition for every crisis-response or risk-management matter.

14. Email, Webinar, and Professional Communications

CrisisRisk may send webinar invitations, educational materials, service information, and other professional communications to insured organizations, prospective clients, insurers, brokers, and other professional contacts.

CrisisRisk currently uses Squarespace email functionality for certain webinar and professional communications.

Where required by applicable law, CrisisRisk will obtain consent or otherwise ensure an appropriate legal basis before sending marketing communications.

Recipients may use the unsubscribe functionality provided in applicable marketing communications.

Unsubscribing from marketing communications does not prevent CrisisRisk from sending necessary operational, contractual, crisis-response, insurance-related, account, licensing, or other non-marketing communications.

15. Microsoft 365

CrisisRisk uses Microsoft 365 for business email and related communications and productivity functions.

Information sent to or from CrisisRisk by email or communicated internally may therefore be transmitted, processed, or maintained using Microsoft services.

16. Service Providers and Other Recipients

CrisisRisk uses third parties to support its business and professional services.

Depending upon the circumstances, recipients or service providers may include:

These organizations may process information to the extent appropriate to their role and the circumstances involved.

- DreamHost
- Microsoft
- Squarespace
- Jotform
- Specialty Answering Service
- Insurers and reinsurers
- Insurance brokers and agents
- Attorneys
- Counselors
- Investigators
- Security professionals
- Crisis-management professionals
- Technology providers
- Consultants and other professional service providers

17. Beazley Portal and Other Third-Party Platforms

Certain CrisisRisk services and resources may be introduced, referenced, or made accessible through websites or platforms operated by insurers or other third parties.

For example, Beazley operates a portal through which eligible insureds may obtain information about CrisisRisk services and may be directed to CrisisRisk tools and resources.

Some CrisisRisk resources referenced or made available through the Beazley portal, including certain proprietary toolkits, are hosted on CrisisRisk.com rather than on the Beazley platform. A user who follows a link or other access path from the Beazley portal to CrisisRisk.com may therefore leave the Beazley-operated environment and interact directly with CrisisRisk.

Where a CrisisRisk toolkit or other proprietary resource is hosted on CrisisRisk.com, CrisisRisk may require the user or the user's organization to establish an account and enter into or accept an applicable license agreement before access is provided. Personal information collected by CrisisRisk in connection with account creation, licensing, authentication, and access is handled in accordance with this Privacy Policy.

Information collected directly by Beazley through a Beazley-operated website or portal is subject to the privacy practices and other applicable terms governing that platform.

Similarly, CrisisRisk uses Jotform to administer certain questionnaires, surveys, and assessments. Information entered into Jotform is processed through that platform and is also received and used by CrisisRisk as described in this Privacy Policy.

Other third-party websites or platforms linked to or used in connection with CrisisRisk services may have their own privacy policies and terms. Users should review the privacy information applicable to those services.

18. International Transfers

CrisisRisk is headquartered and operates in the United States. We do not currently maintain offices outside the United States.

Accordingly, personal information concerning individuals in the EEA, United Kingdom, Singapore, Australia, and other countries may be transferred to, accessed from, processed, or stored in the United States.

Information may also be processed by service providers in the United States or other countries depending upon the provider and service involved.

Where applicable law requires safeguards for an international transfer, CrisisRisk will use an appropriate lawful transfer mechanism or safeguard. Depending upon the jurisdiction and circumstances, these may include adequacy mechanisms, approved contractual provisions, standard contractual clauses, contractual protections, or another mechanism permitted by applicable law.

Where appropriate, CrisisRisk will take reasonable steps to ensure that service providers receiving personal information are subject to privacy and security obligations appropriate to the information and applicable legal requirements.

Individuals may contact CrisisRisk using the information below for additional information concerning international transfers relevant to their personal information and, where applicable, information about or a copy of relevant safeguards.

19. Cookies and Similar Technologies

CrisisRisk.com and its technology providers may use cookies and similar technologies necessary for:

CrisisRisk does not currently represent that it uses behavioral advertising technologies or social-media advertising pixels on CrisisRisk.com.

Because website technologies can change, CrisisRisk periodically reviews its practices and may update this Privacy Policy and any applicable cookie notice when necessary.

Where applicable law requires consent before non-essential cookies or similar technologies are used, CrisisRisk will provide an appropriate consent mechanism.

- Website operation
- Account authentication
- Security
- Session management
- Remembering preferences
- Website administration
- Technical performance

20. Sale of Personal Information

CrisisRisk does not sell personal information.

We do not sell, rent, or exchange client, insured, prospect, questionnaire, crisis-response, account, licensing, or contact information to third parties for their independent marketing purposes.

Disclosure of information to insurers, brokers, attorneys, counselors, service providers, or other parties as necessary to provide services, respond to incidents, administer insurance matters, operate our business, or administer licensed resources is not treated by CrisisRisk as a sale of personal information.

21. Information Security

CrisisRisk uses reasonable administrative, technical, and organizational measures intended to protect personal and confidential information from unauthorized access, use, alteration, disclosure, loss, or destruction.

Access to sensitive CrisisRisk information is intended to be limited to individuals who require access for legitimate business or professional purposes.

No website, email system, cloud platform, internet transmission, or electronic storage system can be guaranteed to be completely secure. CrisisRisk therefore cannot guarantee absolute security.

22. Data Retention

CrisisRisk retains personal information only for as long as reasonably necessary for the purposes for which it was collected and for legitimate business, contractual, insurance, legal, regulatory, security, and professional purposes.

Retention periods vary depending upon the type of information and circumstances.

For example, CrisisRisk may need to retain information to:

When information is no longer reasonably required, CrisisRisk may delete, destroy, anonymize, or otherwise dispose of it consistent with applicable requirements and business practices.

- Provide ongoing services
- Maintain questionnaire and assessment records
- Maintain insurance and client records
- Maintain user-account and restricted-resource records

- Document acceptance of license agreements
- Protect proprietary and intellectual-property rights
- Document crisis-response services
- Support claims or investigations
- Support litigation or anticipated litigation
- Comply with legal holds
- Meet contractual or regulatory obligations
- Resolve disputes
- Establish, exercise, or defend legal or contractual rights

23. EEA and United Kingdom Privacy Rights

Where the EU GDPR or UK GDPR applies, individuals may have rights concerning their personal data, subject to applicable conditions and exceptions. These may include the right to:

Right to Object: Where CrisisRisk processes personal data based upon legitimate interests, an individual may have the right to object to that processing based upon their particular situation. Individuals also have the right to object to processing of their personal data for direct-marketing purposes.

These rights are not absolute. For example, CrisisRisk may be required or permitted to retain information because of an insurance claim, crisis event, investigation, litigation, legal hold, contractual obligation, legal requirement, privilege, security concern, license agreement, protection of proprietary rights, or need to establish, exercise, or defend legal rights.

CrisisRisk may take reasonable steps to verify the identity and authority of an individual making a request.

- Obtain information about the processing of personal data
- Request access to personal data
- Request correction of inaccurate or incomplete personal data
- Request deletion of personal data in certain circumstances
- Request restriction of processing in certain circumstances
- Object to certain processing, including certain processing based upon legitimate interests
- Object to direct marketing
- Receive certain personal data in a portable format where the right to data portability applies
- Withdraw consent where processing is based upon consent
- Exercise applicable rights concerning solely automated decisions having legal or similarly significant effects
- Lodge a complaint with the applicable data-protection supervisory authority

24. Singapore Privacy Rights

Where Singapore's Personal Data Protection Act ("PDPA") applies, CrisisRisk handles personal data in accordance with applicable requirements concerning collection, use, disclosure, protection, retention, and overseas transfers.

Subject to applicable exceptions, individuals may request:

CrisisRisk will evaluate requests in accordance with applicable Singapore law.

Where personal data subject to Singapore's transfer requirements is transferred outside Singapore, CrisisRisk will take steps required by applicable law to provide an appropriate standard of protection.

Questions or requests concerning Singapore personal data may be directed to the privacy contact identified below.

- Access to personal data held by CrisisRisk
- Information regarding certain uses or disclosures of their personal data
- Correction of errors or omissions in their personal data
- Withdrawal of consent where processing depends upon consent

25. Australia Privacy Rights and Complaints

Where Australia's Privacy Act 1988 and the Australian Privacy Principles ("APPs") apply, CrisisRisk will handle personal information in accordance with applicable requirements.

Individuals may contact CrisisRisk to:

A privacy complaint should describe the concern and provide sufficient information for CrisisRisk to investigate it.

CrisisRisk will review privacy complaints and seek to respond within a reasonable period. We may contact the individual for additional information necessary to investigate or respond to the complaint.

Because CrisisRisk is located in the United States, personal information provided in connection with CrisisRisk services may be disclosed to or held by recipients outside Australia, particularly in the United States. Other countries may be involved where a service provider or professional involved in a particular matter operates from another jurisdiction.

Where applicable, an individual may also have the right to raise an unresolved privacy concern with the Office of the Australian Information Commissioner (OAIC).

- Request access to personal information CrisisRisk holds about them
- Request correction of inaccurate, out-of-date, incomplete, irrelevant, or misleading personal information
- Ask questions about CrisisRisk's handling of their personal information
- Make a complaint concerning CrisisRisk's handling of personal information

26. Other Jurisdictions

Individuals located in other jurisdictions may have additional privacy rights under applicable local law.

CrisisRisk will respond to privacy requests in accordance with applicable law and the circumstances of the request.

Nothing in this Privacy Policy is intended to limit a privacy right that cannot lawfully be limited.

27. Children and Minors

CrisisRisk.com and CrisisRisk's services are intended for organizations, insurance professionals, insureds, and other business and professional users. The website is not directed toward children.

CrisisRisk does not knowingly solicit personal information directly from children through CrisisRisk.com.

CrisisRisk may, however, receive information concerning minors in connection with a crisis, threat, insurance claim, school-related matter, investigation, or other professional engagement. Such information is handled in the context of the applicable professional matter and is not collected because CrisisRisk offers services directly to children.

28. No Payment Information Collected Through CrisisRisk.com

CrisisRisk does not currently accept payments or collect credit-card or payment-account information through CrisisRisk.com.

If this practice changes, this Privacy Policy will be updated as appropriate.

29. Changes to This Privacy Policy

CrisisRisk may update this Privacy Policy from time to time to reflect changes in our services, technology, service providers, international operations, business practices, or legal requirements.

When we make material changes, we will post the revised Privacy Policy on CrisisRisk.com and update the effective date above.

30. Contact Us and Privacy Requests

Questions about this Privacy Policy, privacy requests, or concerns about CrisisRisk's handling of personal information may be directed to:

CrisisRisk Strategies, LLC
PO Box 31494
Sea Island, Georgia 31561
United States

Email: crisis@crisisrisk.com

Please include sufficient information for us to understand and respond to your request. CrisisRisk may need to verify your identity or authority before fulfilling certain requests.